CyberStronger

TRAINING LABS

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Additional Scanning Options	**YES**	1 Hour	Students will leverage Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).
Advanced Techniques for Malware Recovery	**YES**	1 Hour	Students will use the SysInternals Suite of utilities to analyze processes, DLLs, registry edits and other auto start functions to locate and remove malicious software from an infected Windows 7 victim machine.
Analysis and Recommendation Report	**YES**	1 Hour	Students will do a Vulnerability Assessment on a network. Students will then analyze the results and place them in a Recommendation Report.
Analyze and Classify Malware	**YES**	1 Hour	In this lab you will attempt to conduct basic analysis on some malware samples that were found on the internal network.
Analyze and Update a Company BCP/BIA/DRP/CIRP	**YES**	2 Hours	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP). Each of these documents are used to address different, but related, aspects of continuing or recovering business functionality during/after an incident. During the course of the lab, students will perform a gap analysis using the provided BCP, BIAs and DRP, and make the necessary fixes to the DRP.
Analyze Browser-based Heap Spray Attack	**YES**	1 Hour	Students will identify a browser-based attack used against a corporate asset using a network protocol analyzer. Students will determine the type of attack used and pinpoint exploit code in network traffic.
Analyze DoomJuice Infection to Identify Attack Vector and Payload	No	1 Hour	Students will use popular system analysis tools on an infected machine in order to identify signs of infection. Afterwards, students will manually remove malware from the system.
Analyze Malicious Activity in Memory Using Volatility	**YES**	1 Hour	Students will use the open source Volatility tool to analyze a memory snapshot and determine what malicious software has infected the victim machine.
Analyze Malicious Network Traffic	**YES**	2 Hours	Students will take some time to review malicious traffic within a controlled environment. Using Wireshark and some pointers from a previous technical report on the FlashPack Exploit Kit, they will focus their attention on finding (in two traffic captures) evidence of when and how a victim system was infected with the exploit kit.
Analyze Packed Executable to Identify Attack Vector and Payload	**YES**	1 Hour	Students will use a handful of tools to analyze a provided suspicious file. Using CFF Explorer, they will modify how the suspicious program stores variables in memory, detect what packer it was packed with, unpack that file and then save it in an unpacked state. Using ExeinfoPE, they will double-check and ensure that the processed version of the program has been successfully unpacked. The students will then run the suspicious program while Process Hacker is running and then dump all strings associated with the suspicious process to a text file. Using the dumped strings they will piece together what the program was designed to do.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Analyze SQL Injection Attack	**YES**	1 Hour	Students will Identify the use of an SQL Injection through the use of Wireshark. The students will also isolate the different aspects of the SQL Injection and execute the selected code.
Analyze Structured Exception Handler Buffer Overflow Exploit	**YES**	1 Hour	Students will identify the use of a Buffer Overflow exploit through the use of Wireshark and by analyzing items found in the captured traffic. The students will also find the exploit code and isolate the different aspects of a Buffer Overflow exploit.
Analyze Various Data Sources to Confirm Suspected Infection	**YES**	1 Hour	Students will review network traffic to confirm the presence of malicious activity using various tools including Wireshark and VirusTotal.com.
Applying Filters to TCPDump and Wireshark	**YES**	1 Hour	This lab exercise is designed to allow the trainee to become familiar with applying a capture filter to TCPDump and Wireshark using Berkley Packet Filter (BPF) syntax.
Assembly Language Fundamentals	No	4 Hours	Competency in assembly is critical across a variety of development and information security professions ranging from reverse engineers and malware analysts to firmware and exploit developers. DEV540 provides students with a strong foundation in assembly language programming and the architectures for x86 and Intel64 processors. Students who take this course will use the Microsoft Macro Assembler (MASM) and Netwide Assembler (NASM) to create a variety of binaries, to include shellcode, during the course. Attendees are strongly encouraged to take DEV400 (Intro to Programming C) or have basic programming experience in C/Java, knowledge of networking concepts and basic OS functionality like processes, threading, and memory management prior to taking this class.
Assess A High-Risk System	**YES**	1 Hour	Systems that are required to provide remote or public customer access should be placed in a Demilitarized Zone (DMZ). The DMZ is a separate space set aside for public access but does not allow attackers access to sensitive internal network assets. If public-facing (Internet) servers were hosted on the internal network then an attacker could easily breach the server and use trust relationships or configurations to burrow further into the internal network.
Assessing Vulnerabilities Post Addressal	**YES**	1 Hour	Students will use Snorby against multiple systems to identify and mitigate any vulnerabilities found.
Auditing Service Accounts	**YES**	1 Hour	Students will audit service accounts in a Windows Server environment. They will note the services that are running with the help of the server Administrator account and make necessary corrections to them. The corrections will minimize the chance of a successful attack against those services allowing for privilege escalation attempts, leveraging the associated service account, from going anywhere.
Auditing Service Accounts and Creation of Service Accounts To Run Specific Services	No	1 Hour	Students will explore the auditing of service accounts in a Windows Environment. Students will then replace services running with the administrator account with accounts that are appropriate for that running service.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Auditing Service Accounts and Setting Up Automated Log Collection	**YES**	2 Hours	Students will perform a check on accounts and services running on a server to ensure they are set to the appropriate levels – ensuring legitimate accounts and processes are being used. They will also set up automated log aggregation on the same server, and a network firewall, to ensure system changes and logs are sent to a remote archiving server for future use during incident response events.
Automated in-Depth Packet Decoding	No	2 Hours	Students will use Network Miner to analyze network traffic.
Automated Vulnerability Assessments	No	1 Hour	Students will use Core Impact to conduct an automated vulnerability scan of specific systems in order to identify potential threat vectors.
Backup and Restore Data in Windows	No	2 Hours	In this lab students will backup and restore data by creating files and folders, backing up that data, and finally restoring the lost data using the Windows Server Backup tool.
Baseline Systems in Accordance with Policy Documentation	**YES**	1 Hour	Students are provided a whitelist of applications allowed for installation on a system. Students will compare the list against multiple hosts and remove the installed applications which are not on the list.
Basic Linux x64 Binary Exploitation with pwntools	No	1 Hour	In this lab, we will look at some basic binary exploitation in 64 bit Linux. We will be looking at assembly code as part of the exploit development process. You don't need to be an expert with assembly code, and we will be explaining all the code that we examine.
Basics of Metasploit	**YES**	1 Hour	In this lab we will dive into exploiting machines in our test environment. Some of the machines in this network are easy to exploit, and some are a bit more challenging. Throughout the process, we will walk through how to use Metasploit and a few additional tools to gather information and exploit the vulnerabilities.
BCP DRP and Test Planning	**YES**	4 Hours	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA) and Disaster Recovery Plan (DRP). During the course of the lab, students will perform a gap analysis on the provided BCP, BIAs and DRP, and make the necessary fixes to those documents. After revising the previous documents the students will create a test for the covered assets, procedures and personnel.
BitCoin Mining Web Application on Corporate Network	No	1 Hour	Students will identify unauthorized activity on a corporate network. Students will then identify what type of cyber incident may have occurred and determine the attack vector. Finally, Students will collect information on the incident in order to prepare an Incident Response report.
BitLocker Setup	No	1 Hour	This lab shows the student how to setup BitLocker on a Windows 8.1 Professional system.
Block Incoming Traffic on Known Port	**YES**	1 Hour	In this lab, the student will respond to an incident by blocking incoming traffic on a known port from a specific IP.
Centralized Monitoring	No	1 Hour	In this lab you will manually upload log data to Splunk. You will also configure Splunk and linux syslog to automate the process of centrally locating log data.
Check for Indicators of Other Attack Activity (Debug PE File)	No	2 Hours	Students will check for indications of other attack activity.
CIRP Creation After Cyber Attacks	**YES**	1 Hour	With the help of a template and a good deal of supporting documentation, students will create a Computer Incident Recovery Plan.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
CIRP Creation and Disaster	**YES**	2 Hours	Students will become familiar with the creation of a Cyber Incident Response Plan (CIRP). During the course of the lab, the student will also run through a table-top run simulated cyber incident which will help them validate the earlier changes made to the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), as well as the newly created CIRP.
CIRP Creation and Review of BCP and DRP	**YES**	2 Hours	Students will become familiar with the creation of a Cyber Incident Response Plan (CIRP). During the course of the lab, the student will also run through a table-top run simulated cyber incident which will help them validate the earlier changes made to the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), as well as the newly created CIRP.
Client Side Exploitation with Social Engineering	**YES**	1 Hour	In this lab you will practice a social engineering attack, performing actions as both the attacker and as the victim, in order to demonstrate how a simple phishing attack looks, and how easy it is to fall victim to one.
Clonezilla_Network	No	1 Hour	As a incident responder, it's important to understand how to create baseline templates. You will learn how Clonezilla may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WDS.
Collecting Logs and Verifying Syslog Aggregation	**YES**	2 Hours	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the pull method (where the logging device itself pulls the logs off target devices). This lab will deal with the most common method, pull method, used today in log aggregation, that is, ie. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.
Command-Line Python	No	2 Hours	Python for Network Security Administrators is an introductory Python course weighted toward security and networking topics. The course exposes students to common Python types, data manipulation, networking, command-line scripting, and parallel processing. This course introduces students to programming with Python, and upon completion, students will be able to script common security and networking functions.
Comparing Controls	**YES**	1 Hour	Students will evaluate policies in place on a domain and apply those policies in accordance to organizational standards.
Comprehensive Threat Response	**YES**	2 Hours	In this final lab, we will attempt to exercise all the relevant skills found in this domain. We are focusing on responding to incidents and the skills needed to address these sorts of problems at a practitioner level.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Compromise Assessment with Crowd Response	**YES**	1 Hour	In this lab students will run Crowd Response to conduct an incident response that will generate incident response files that can be analyzed and used to conduct compromise assessment. Crowd Response is a part of a suite of tools sold by crowdstrike.com. The Crowd Response component if free and can replace the traditional response tools by SysInternals and is a good alternative.
Conduct Baseline Comparison for Indicators of Compromise	No	1 Hour	Learners will create a system baseline operating snapshot using the Window Forensic Toolchest (WFT) and compare it against a previously created baseline using the KDiff3 application to identify any deviations from the known-good baseline.
Conduct Log Analysis and Cross Examination for False Positives	**YES**	1 Hour	Students will confirm the validity of event-data analysis to eliminate false-positive events.
Conduct Root Cause Analysis for System Crashes	**YES**	2 Hours	Students will use utilize a specially loaded system to conduct analysis on a captured memory dump from a machine suffering from repeating system crashes. Using a memory analysis tool the students will walk through the process of discovering what is running on the affected system and why these odd behaviors are causing the crashes. This lab will foster tool familiarization and will provide the students with another layer of detail on how the Windows kernel interacts with memory, as well as the various processes invovled.
Conduct Supplemental Monitoring	No	1 Hour	In this lab you implement supplemental monitoring solutions on a network using various Microsoft security tools and built-ins.
Configure a Local Security Policy on Server 2019	No	2 Hours	In this lab students will configure account policies, then local user account settings. Finally the students will manage auditing for user logon events and set user rights and security options.
Configure and Test the Firewall in Windows	No	2 Hours	In this lab the students will configure the Windows Firewall. First they will display the firwall settings and then configure it to permit traffic. Next the students will use PowerShell to configure the firewall and add the FTP service. Finally they will configure the firewall for FTP connections and then display firewall log file information.
Configure Network Load Balancing for a Web Farm	No	2 Hours	In this lab the students will configure network load balancing in a network that contains two web servers. First they will install Internet Information Services (IIS) on the web servers. Next they will install load balancing using PowerShell and then they will configure the load balancer to balance network traffic to the web servers in the web farm. Finally, the students will create custom load balancing rules and verify the traffic is being balanced according to the created rules.
Configure Security Settings by Using Microsoft Group Policy	No	2 Hours	In this lab students will will use Microsoft Active Directory to ensure that domain-joined computers adhere to organizational security policies. They will configure computer and user settings in the Default Domain Policy Group Policy Object (GPO).

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Configure Standard Windows Permissions	No	2 Hours	In this lab students will configure access to files and folders. Fist they will display resource permissions and then configure those permissions using File Explorer. Then they will use PowerShell to configure file and folder permissions. Finally the students will use the icacls utility to configure file and folder permissions.
Configure Update Management in Windows	No	2 Hours	In this lab students will manage Windows updates as a Windows Server Administrator. First they will enable the Windows Update service using PowerShell, then they will display the default Windows Update settings. Then they will review the installed updates using command prompt and the Windows Management Instrumentation WMI) tool. Finally the students will configure automatic updates using Group Policy.
Configure Windows Defender on a Windows System	No	2 Hours	In this lab the students will confirm that the Windows Defender service will block a potentially harmful software. First the students will verify that the Windows Defender service is running. Next they will prevent Windows Defender from scanning folders in which potentially harmful software may be stored. Then they will observe the effect of scanning and exclusions by using Windows Defender. Finally they will permit Windows Defender to remove potentially harmful software.
Configure Windows Firewall ACL Rules	No	2 Hours	In this lab the students will configure inbound and outbound firewall rules to control traffic for a specific server. The students will use the GUI to configure firewall rules, and then use PowerShell to manage firewall rules.
Control Assessment and Evaluation	**YES**	1 Hour	Students are provided a list of controls and a system. They are to ensure that the controls that are provided in the documentation are present on the system.
Core Impact Vulnerability Scan	**YES**	2 Hours	This exercise will introduce students to the advanced settings within the Core Impact. Students will modify scan settings to perform different types of scans and to learn about the different functionalities Core Impact provides. Students will then compare the results of a Core Impact scan to the results of a port scan against the same target and discuss the differences and similarities between the two tools. Lastly, students will use the reporting feature to generate Core Impact reports.
Core Impact Web Application Penetration Testing	**YES**	1 Hour	This lab introduces students to the web application penetration testing suite within the Core Impact application.
Create Custom Snort Rules	**YES**	1 Hour	You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators.
Creating a Baseline Using the Windows Forensic Toolchest (WFT)	**YES**	1 Hour	Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Creating a Case in Autopsy	YES	2 Hours	In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy.
Creating a Case in FTK	YES	2 Hours	In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of FTK.
Creating a Case in OSF	YES	1 Hour	In this lab students will become familiar with creating a lab in OSForensics. Students will also become familiar with the use of OSForensics.
Creating a Forensic Image	YES	1 Hour	Students will create an image of media using FTK Imager.
Creating a List of Installed Programs, Services and User Accounts from a WIN2K12 Server	YES	1 Hour	Students will create a list of installed programs, services, and accounts in a Windows 2012 server environment using various tools and methods.
Creating a Secondary Baseline and Conducting Comparison	YES	1 Hour	Students will create a second baseline using the Window Forensic Toolchest (WFT) and compare it against a previously created baseline using KDiff3.
Creating Recommendations Based on Vulnerability Assessments	YES	1 Hour	Students will use nmap and OpenVAS / Greenbone Vulnerability Scanner to confirm old vulnerable systems and discover new ones. They will perform a risk analysis of the findings and determine steps to be taken to mitigate the issues discovered. Finally, armed with a previously completed audit report as an example, they will fill out the necessary audit documentation to provide details on their findings and any suggested mitigations.
Creating SIEM Reports with Splunk	YES	1 Hour	Students will walk through the creation of SIEM reports using the SPLUNK tool.
Creation of BCP and DRP	YES	3 Hours	Students will be required to create two documents: a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). Both documents deal with worst case scenarios concerning how to keep business going despite the occurrence of a natural disaster, catastrophic accident or serious man-made incident.
Creation of Standard Operating Procedures for Recovery	YES	1 Hour	Students will have access to the results of a vulnerability scan run again a sample Windows 2008 Server. They will perform any necessary remediations to the server by applying a variety of patches, systems/firewall tweaks in order to further harden it. Next, they will run a follow-up scan to ensure that the previously discovered weaknesses have been mitigated down to a reasonable level of risk. After the verification scan has been completed, they will then author a Standard Operating Procedure to help others walk through the same mitigation process they went through - enabling others to perform the same actions on other Windows 2008 servers.
Cryptography: Attacking Classic Ciphers	YES	2 Hours	Training on how to use GPG with a GPG challenge at the end.
Cryptography: Breaking Repeated Key XOR Cipher	YES	4 Hours	This lab walks students through how to attack a repeated key XOR cipher, and then provides a challenge to the student in the form of a fixed plaintext encrypted with a random key. Submitting the key and receiving confirmation constitutes success for this lab.
Cryptography: Breaking Weak RSA Keys	YES	1 Hour	Students will be shown various tools for attacking and using RSA public key information. They will then be given a weak public key and required to break it and decrypt a secret message.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Cryptography: Decrypting Files With a Dictionary Attack	**YES**	2 Hours	Students are given two files and are charged with decrypting both.The first one has the password given, and the second they must brute force the password with a dictionary attack.
Cryptography: Forging Digital Signatures	**YES**	5 Hours	Students will be given an ElGamal Signature Oracle and charged with recognizing an insecure use of it, and exploiting that to calculate the private key. Once the private key is obtained, they will need to create a signature on a given message using that private key.
Cryptography: Forging MACs With Side Channels	**YES**	2 Hours	Students will be faced with a MAC protocol and they must exploit a timing side channel information leak to forge a MAC on a message.
Cryptography: Hidden Veracrypt Containers	**YES**	2 Hours	Students will be shown how to create Veracrypt encrypted containers and will be challenged with creating a hidden container which contains provided files.
Cryptography: Man In the Middle Attack	**YES**	2 Hours	Students will be placed in the middle of an encrypted chat session. They will be able to analyze the protocol, find the flaws, formulate an attack, and execute the attack.
Cryptography: Password Cracking	**YES**	1 Hour	Training on how to use GPG with a GPG challenge at the end.
Cryptography: Setting Up HTTPS in Windows and Linux	**YES**	2 Hours	Setting up HTTPS enabled Web Servers in Linux and Windows
Cryptography: Setting Up Two Factor Authentication	**YES**	2 Hours	Set up 2FA in Windows and Linux
Cryptography: Steganography	**YES**	2 Hours	In this lab, students will learn: How information can be hidden in cover files. How to recognize and search for hidden information. How to steganalyze a file to identify that message was hidden inside.
Cryptography: Using GPG for Encryption and Key Management	**YES**	1 Hour	Training on how to use GPG with a GPG challenge at the end.
Cryptography: Using the OpenSSL CLI Tool	**YES**	2 Hours	Training on how to use OpenSSL CLI tool with a challenge at the end.
CTF Environment	**YES**	8 Hours	This lab hosts a set of CTF challenges that will be automatically scored.
Cyber Security Evaluation Tool (CSET)	No	5 Hours	In this lab students will learn to use the Cyber Security Evaluation Tool (CSET) to evaluate the security posture of an enterprise environment. This will arm the student with knowledge of how to better secure their environment.
Cybersecurity Testing with Core Impact	**YES**	1 Hour	Students use Core Impact to enumerate a local area network and discovery vulnerable machines through a vulnerability scan. Based on the results of the vulnerability scan, students use Core Impact to conduct a penetration test against a previously identified vulnerable machine. Finally, students use the reporting mechanism built into Core Impact to create a host-based assessment outlining the entire vulnerability/penetration test process with a focus on possible remediation actions.
Data Backup to Prep for Recovery	**YES**	1 Hour	In this lab we will simulate the recovery phase where we must perform a backup in a server environment.
Data Downloads and Validation	No	1 Hour	In this lab, students will learn to validate downloads to mitigate risk. Data validation, also known as input validation, a method of ensuring that incoming data is uncompromised before it is allowed to be processed. During transmission on the wire... programs, applications, and services can be corrupted. Data validation employs one or several checks, routines, and rules to ensure that the data coming into a system is meaningful, accurate, and secure.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Data Recovery with Autopsy	**YES**	1 Hour	Students will ingest and process a previously acquired forensic image using Autopsy. The focus of the lab will be on recovering data from the image, reviewing the supplied forensic report and verifying that the image is forensically sound.
Denial of Service PCAP Analysis	**YES**	1 Hour	The student will act as attacker and defender in this scenario. They will receive experience using a custom denial of service python script, and then will switch over to the defensive side. On defense they will need to detect the activity, design firewall rules to block the DoS, implement the rules and then check their effectiveness.
Detect Embedded Shellcode in a Microsoft Office Document	No	1 Hour	Malware can take many forms. Microsoft Office documents can act as a vehicle for a variety of ingenious attacks. Students will detect shellcode embedded in a Microsoft document.
Detect the Introduction of a Malicious Application	**YES**	1 Hour	In this lab, the student will simulate the download of a malicious file from a website. They will then learn how to detect the introduction of malicious programs on a Win7 machine using Microsoft Security Essentials.
Detect Unauthorized Changes by Comparing to Approved Configurations	**YES**	2 Hours	Students will use a variety of tools to record and snapshot different aspects of a Windows workstation, and then compare those recent state updates to approved configurations. The goal is to have them learn to detect and recognize unauthorized changes or deviations to this workstation.
Detecting Changes to System Configurations	**YES**	1 Hour	Students will use a couple of the popular Sysinternals Suite tools to observe configuration changes on a known good/clean system. The scenario will have them perform a running system snapshot using Regshot, TCPView, ListDLLs, Process Explorer and Process Monitor prior to executing a suspicious program. After execution, they will run the same tools, compare the results and note any differences. This lab fosters tool familiarization and will provide an "under the hood" perspective of a running Windows environment.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Dev0 - Introduction to Windows Socket Programming in C/C++	No	2 Hours	Welcome to DEV 0, Welcome to Intro to Windows System and Socket Programming with C/C++. In this course you will learn the basics of programming in C which will give you the needed foundation to progress on to Windows System and Socket Programming with the Windows API. We will strive to keep the lecture portions of this course to what we feel is the minimum needed to give you a good grounding in the concepts needed to write programs in C. As we progress through the class we will do our best to employ the Socratic method of teaching whereby we won't necessarily always tell you the answer rather we will provide you with core information and ask you to think and employ logic, problem solving and other skills to create the answer. However, if you're stuck and if you've given a good effort at trying to find an answer or solve a problem, please ask the instructor. With that in mind if the topic you wish to discuss falls outside of the scope of the course learning objectives, we may ask you to revisit the question on break or after other students don't need any further assistance.
Disable User Account on Windows 10	**YES**	1 Hour	In this lab, the student will respond to a suspected insider threat incident by disabling user accounts in Windows. Additionally, the student will learn to search for and conduct basic analysis on suspected malicious events via the mmc Event Viewer snap-in.
DLL Editing	No	1 Hour	This exercise will demonstrate the functions of Dynamic Link Libraries (DLLs). Upon completing this exercise, the trainee will have a better understanding of how DLLs affect the user's ability to run various programs.
DNS as a Remote Shell	No	1 Hour	This lab exercise is designed to allow the trainee to become familiar with recognizing remote shells that operate using well known ports such as DNS.
Dynamic Malware Analysis	**YES**	1 Hour	Students will use utilize two virtual machines, inside a protected network, to observe configuration changes on a known good / clean system and all of the unusual network traffic generated by the suspect software they will be analyzing. On the clean system they will use Regshot, Argon Network Switcher, Process Hacker, Process Monitor and Noriben to gather details on what the suspicious program is actually doing. On another support machine they will set up a fake DNS server to receive all suspicious traffic, and pass that traffic over to Wireshark for further analysis. This lab will continue to foster tool familiarization and will provide the students an introduction to capturing network traffic by using a simple "man-in-the-middle" system.
Entering Information into a CMDB	**YES**	1 Hour	Students will review an old asset list and enter all of the contained information into a Configuration Management Database (CMDB). Students will then gather information from two systems (a Windows and Linux system) and add that data into the same CMDB.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Evasive Maneuvers and Post Exploitation	**YES**	1 Hour	In this lab, you will practice enumeration of outbound egress policy, which is necessary when attempting to perform reverse connections, or exfiltrate data.
Event Log	No	1 Hour	In this lab, the trainee will have the opportunity to review event log files associated with the Windows 7 operating system.
Event Log Collection with QRadar	**YES**	1 Hour	In this lab you will use QRadar with wincollect to ingest logs from a local host for analysis
Event Log Collection with Splunk	**YES**	2 Hours	In this lab you will use Splunk Enterprise to ingest logs from a local host for analysis
Event Logs with Autopsy	**YES**	1 Hour	Students will learn what Event Logs are, how to view them, and what kind of information can be found in them.
Firewall Setup and Configuration	**YES**	1 Hour	In this lab you will perform the steps necessary to set up a pfSense firewall from the basic command line interface and then configure the firewall using the web configuration GUI on a Windows machine. This lab will provide an understanding how network interfaces are configured to allow network connectivity. You will also view and create a firewall rule which enforces your understanding of how network traffic can be managed at different levels – (IP-based, Protocol-based, Machine-based, etc).
Fixing a Company BCP, DRP and CIRP	**YES**	2 Hours	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP). During the course of the lab, students will perform a gap analysis using the provided BCP, BIAs and DRP, and make the necessary fixes to the DRP.
Force Point DLP Email Overview	**YES**	1 Hour	Forcepoint DLP will teach the student how to configure Forcepoint DLP to stop data loss on the email channel.
Force Point DLP Network Overview	**YES**	1 Hour	DLP network: Monitors and enforces DLP policies across several communication channels, including email, web, IM, network printing. This lab will focus on securing these channels from data loss.
FTK Analysis & Reporting	No	1 Hour	The FTK Imaging & Analysis lab is focused on building incident handling skills. FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence . This lab will take the student through an overview of FTK Imager.
FTK Enterprise Fundamentals and Mobile Investigation	No	2 Hours	In this lab, students will gain a deep understanding of the FTK enterprise edition user interface. Students will also sharpen their incident handling skills while investigating real-world scenarios. Students will also use their incident handling skills to investigate mobile device information using FTK enterprise.
Fundamentals of Exploit Development	No	3 Hours	Exploit Development

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Fundamentals of Malware Analysis	No	1 Day, 16 Hours	NOTE: This lab requires the following textbook: "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig". MAL400 exposes students to the theoretical knowledge and hands-on techniques used to analyze malware. In MAL400, students will learn how to identify and analyze software that causes harm to users, computers, and networks. Students will dissect malware and learn how to identify it, how it works, and how to defeat it. The course begins with an overview of the malware analysis process followed by dynamic analysis, assembly, and an introduction to debuggers and disassemblers.
Gap Analysis of Firewall Rules	**YES**	2 Hours	Students will log into an organization's firewall, document existing firewall rules, analyze these rules and making recommendations based on this analysis. Students will then make make the necessary changes.
Hardening C#.NET Web Apps - Broken Access Control	No	1 Hour	In this lab, we will show an exploit on a user's cookie, then apply remediation measures, and then reattempt the exploit.
Hardening C#.NET Web Apps - Broken Authentication	No	1 Hour	This lab teaches methods to secure the authentication methods in a web application written in C#.
Hardening C#.NET Web Apps - Cross Site Scripting	No	1 Hour	This lab teaches methods to secure web applications written in C# against XSS attacks.
Hardening C#.NET Web Apps - CSRF	No	1 Hour	This lab teaches methods to secure web applications written in C# against Cross Site Request Forgery attacks.
Hardening C#.NET Web Apps - File Uploads	No	3 Hours	This lab teaches methods to secure web applications written in C# with respect to file upload capabilities.
Hardening C#.NET Web Apps - OS Command Injection	No	1 Hour	This lab teaches methods to secure a web application written in C# against OS Command Injection attacks.
Hardening C#.NET Web Apps - Password Hashing	No	1 Hour	This lab teaches how to properly use password hashing in a C# web application.
Hardening C#.NET Web Apps - Secure Deserialization	No	1 Hour	This lab teaches methods to secure web applications written in C# against Insecure Deserialization attacks.
Hardening C#.NET Web Apps - SQL Injection	No	1 Hour	This lab teaches methods to secure a web application written in C# against SQL Injection attacks.
Hardening C#.NET Web Apps - Two Factor Authentication	No	1 Hour	This lab teaches how to deploy Google Authenticator in a C# web application in order to deploy Two Factor Authentication.
Hardening C#.NET Web Apps - Web Configuration	No	1 Hour	This lab teaches methods to secure the C# configuration for web applications written in C#.
Hardening C#.NET Web Apps - XXE	No	1 Hour	This lab teaches methods to secure a web application written in C# against XXE attacks.
Hash Verification	**YES**	1 Hour	Students will understand and use hash verification to identify and compare files and forensic images.
Holistic Network Identification and Protection	No	2 Hours	This exercise provides students an opportunity to exercise their network identification and protection capabilities learned in the last week. They are responsible for identifying and leveraging the appropriate tools (of those provided) to identify all components of the network and assess it for potential vulnerabilities.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Host Data Integrity Baselining	No	1 Hour	This lab takes the trainee into basic concepts regarding establishing baselines of files and directories with Kali Linux and Windows 7. In the first part of the lab, the trainee will establish a baseline of the passwd file within Kali Linux, and in the second part the trainee will establish a baseline of the C:\> drive within Windows 7.
Host Identification Scanning via Windows	No	1 Hour	Students will leverage Scanline, a Windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).
Host Identification Scanning with Linux	**YES**	1 Hour	Students will utilize Nmap, a network discovery and mapping tool to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as routers.
Identify Access to a LINUX Firewall Through SYSLOG Service	**YES**	1 Hour	Students will identify access to a PFSENSE firewall through the forwarding of SYSLOG (System logs) from a Firewall to the SYSLOG service we have configured and set up on the Network. Students will then identify malicious activity through system logs.
Identify and Remove Trojan Using Various Tools	**YES**	1 Hour	Students will detect malicious files and processes using various tools. Students will then remove the malicious files and/or processes.
Identify Rootkit and DLL Injection Activity	**YES**	1 Hour	Students will use Olly Debugger to debug a suspect program and determine if any of the observed behavior is malicious or not. They will also use Process Hacker to confirm if a possible DLL injection was successful. This lab fosters an understanding of debuggers, shows one possible way malicious software hooks into legitimate programs and will provide an "under the hood" perspective on how programs work in the Windows environment.
Identify Suspicious Information in VM Snapshots	No	1 Hour	Students will identify known IOCs for Stuxnet and save them for analysis. Students will then identify malicious drivers associated with the malware, and identify AES keys in memory.
Identify Whether High-Risk Systems Were Affected	**YES**	1 Hour	The highest risk systems are the ones with Internet facing Applications. One an attacker from the Internet is able to compromise the internal network, then it is very likely they will attempt to move to other machines on the network. The machines in the Demilitarized Zone (DMZ) are at high risk because they are not usually as protected as the computers which are part of the Internal Network.
Identifying Anomalous ARP	No	1 Hour	This lab exercise is designed to allow the trainee to become familiar with identifying anomalous ARP traffic.
Identifying Intrusion and Mitigating Attacks with RHEL Server	No	1 Hour	This last lab is similar to the Windows Incident Response lab, but different in that this one requires you to run through the IR process in a Linux, more specifically a Red-Hat, environment. The same IR methodologies and procedures apply in both environments; these include identifying any security-issues and their scope, containing the issues as best as possible, removing any present threats if found, recovery, and report-generation. Making sure you account for all of these is the key to sound IR work.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Identifying Key Assets	**YES**	1 Hour	Students will use nmap to identify specific assets on their network.
Identifying Malicious Callbacks	**YES**	1 Hour	Students will try to identify suspicious behavior on a compromised machine using volatility. Students will then look at processes, parent processes, connections, unlinked DLLs, and malicious kernel callbacks that are associated with suspected malware.
Identifying Malicious Network Connections	**YES**	1 Hour	When investigating a cybersecurity incident it's important to take memory snapshots of affected systems for further analysis. Students will conduct analysis and look for malicious network connections, processes, and other artifacts.
Identifying System Vulnerabilities with OpenVAS	**YES**	2 Hours	Students will scan a system in OpenVAS (Open Vulnerability Assessment) to discover and identify systems on the network that have vulnerabilities.
IDS Setup and Configuration	**YES**	1 Hour	Network and host based Intrusion Detection Systems (IDS) analyze traffic and provide log and alert data for detected events and activity. Security Onion provides multiple IDS options including Host IDS and Network IDS. In this lab you will setup Security Onion to function as a network based IDS and Snorby, the GUI web interface for Snort.
Implement Single System Changes in Firewall	No	1 Hour	In this lab you will make changes to the PFSense Firewall in order to block specific ports and types of traffic.
Implementing Least-Privilege on Windows	**YES**	1 Hour	Least-privilege is an important concept across many domains (e.g., Windows server/workstation management, networking, Linux management, etc.) and requires great discipline to implement properly. This lab walks students through implementing least privilege in both an Active Directory setup and a normal Windows-based workstation.
Incident Detection and Identification	No	3 Hours	Students will demonstrate their capabilities to identify network components and detect a potential incident. **NOTE** This is a scenario-based lab. Students receive minimal guidance intentionally. This lab reflects environments similar to the certification environment.
Install EMET and Edit Host Files	No	1 Hour	In this lab the student will install Microsoft's Enhanced Mitigation Enhanced Toolkit (EMET) and edit the the computer's /etc/host file to redirect a system to localhost for the purposes of DNS sink-holing.
Install and Manage Windows Admin Center Extensions	No	2 Hours	In this lab the students will install and configure Windows Admin Center while also managing extensions. First they will install the Windows Admin Center, and then extensions on the Windows Admin Center server. Finally they will use PowerShell to install and uninstall additional extensions.
Installing Patches and Testing Software	No	2 Hours	Students will identify if a vulnerability is present in the systems and remediate the vulnerability if necessary.
Internet History	**YES**	1 Hour	In this lab, students will look at how to find and identify internet history in a forensic image.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Interoffice Communications Correction	No	1 Hour	Students will identify an inoperable office chat client and fix the issue. The student will then identify a rogue server on a system.
Intro To Linux - Backing Up, Compression, and Scheduling	**YES**	1 Hour	In this lab we will consider tools that can be used to backup your data. In covering this, we will also look at compression tools and scheduling, which can be used in conjunction with backups to achieve efficient and regular backups.
Intro to Linux - Bash Scripting	**YES**	3 Hours	In this lab, you will learn how to write simple programs in Bash. There are many different shells available in Linux that have different features. The features we will cover are specific to Bash.
Intro To Linux - Command Line Basics	No	1 Hour	In this lab, you will learn a variety of commands that are useful to know when navigating the Linux command line interface.
Intro To Linux - File Systems	No	1 Hour	In this lab, we will learn about how the file system is organized in a Linux Operating System, and the location of some of the more important files and directories.
Intro To Linux - Installing Software	**YES**	2 Hours	In this lab, we will learn about how to install and update software, both manually, and also with the distribution's package manager. We will focus on two package managers in particular, apt and yum.
Intro To Linux - Kernel	**YES**	1 Hour	In this lab, we will look at the Linux Kernel. We will cover kernel modules, custom kernel compilation, kernel configuration tuning, and system commands.
Intro To Linux - Networking Tools	**YES**	1 Hour	In this lab, we will look at the different networking tools in Linux and how to configure networking.
Intro to Linux - Pipes and Filters	**YES**	2 Hours	In this lab, you will learn how to chain multiple commands together to achieve more complex goals. You will also be exposed to regular expressions and how they can be used in combination with pipes and filters.
Intro To Linux - Processes and Booting	**YES**	1 Hour	In this lab, we will learn how to work with processes in Linux and how the system boots up and the services are managed. Newer versions of Linux use systemd to manage the services, and older versions use System V, and we will look at both.
Intro to Linux - Routing and SSH Tunnels	**YES**	2 Hours	Routing is an important networking concept. Routing is typically done by dedicated routers, but can also be done by host systems, such as pfSense or even a regular Linux machine. In a production network, you would likely not use a Linux machine to perform routing, but by experimenting with routing on Linux, you can gain a deeper understanding of how it works and how to configure it.
Intro To Linux - Sed and Awk	**YES**	2 Hours	In this lab we will learn how to use some of the more useful parts of Sed and Awk. These two tools are incredibly powerful and can greatly improve your ability to function effectively in a Linux command line environment.
Intro To Linux - Text Editors	**YES**	1 Hour	In this lab, we will learn how to edit basic text files from the command line, as well as a GUI tool for the same. Text files are very common in Linux and are used often for storing data as well as configuration information. Being able to edit these files is of vital importance and if you use Linux regularly, will be a common task.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Intro To Linux - Users and Groups	**YES**	1 Hour	In this lab, we will look at managing users on a Linux system. In particular, we will cover how to create, modify, and delete users and groups. We will also look at how to assign a file a user and group, and how the basic permissions work in Linux.
Intro to Python	No	2 Hours	This lab is a quick introduction to programming in Python. It assumes that you already understand how to program. The goal is to give you a quick familiarity to Python or refresh older knowledge.
Introduction To OWASP Top Ten: A1 - Injection	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A1: Injection.
Introduction To OWASP Top Ten: A10 - Insufficient Logging and Monitoring	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A10: Insufficient Logging and Monitoring.
Introduction To OWASP Top Ten: A2 - Broken Authentication	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A2: Broken Authentication.
Introduction To OWASP Top Ten: A3 - Sensitive Data Exposure	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A3: Sensitive Data Exposure.
Introduction To OWASP Top Ten: A4 - XML External Entities	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A4: XML External Entities.
Introduction To OWASP Top Ten: A5 - Broken Access Control	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A5: Broken Access Control.
Introduction To OWASP Top Ten: A6 - Security Misconfiguration	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A6: Security Misconfiguration.
Introduction To OWASP Top Ten: A7 - Cross Site Scripting	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A7: Cross Site Scripting
Introduction To OWASP Top Ten: A8 - Insecure Deserialization	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A8: Insecure Deserialization.
Introduction To OWASP Top Ten: A9 - Using Components With Known Vulnerabilities	**YES**	1 Hour	This module for the Introduction to OWASP Top Ten Module covers A9: Using Components With Known Vulnerabilities.
Introduction to Squert	No	1 Hour	In this lab, you will learn how to use Squert to view previously generated event data detected by the sensors.
Leveraging Internal Intelligence Resources (v.2023)	**YES**	1 Hour	Students will leverage Zenmap and Tenable Nessus vulnerability scanner to perform an internal scan of networked resources. They will, in turn, use the intelligence they gather about these scanned systems to evaluate the security posture of the devices on the network.
Linux Analysis	**YES**	1 Hour	Students will use a given image to become familiar with where to find forensically interesting items in a standard Linux distribution.
Linux Exploitation	**YES**	1 Hour	During this lab, you will use scanning and enumeration techniques to explore vulnerable services on two different Linux servers.
Linux Familiarization Lab	**YES**	1 Hour	Lab to familiarize students to Linux.
Linux Routing	No	2 Hours	Routing is an important networking concept. Routing is typically done by dedicated routers, but can also be done by host systems, such as pfSense or even a regular Linux machine. In a production network, you would likely not use a Linux machine to perform routing, but by experimenting with routing on Linux, you can gain a deeper understanding of how it works and how to configure it.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Linux x64 Binary Exploitation with ASLR and PIE	No	2 Hours	The final two exploit mitigation techniques that we will discuss deal with the randomization of the executable. In the labs up to this point, we knew ahead of time where certain things would be located. The exception to that was the stack, which could be somewhat unpredictable simply because you may not know the internal state of the program and thus not know how many frames are present on the stack. The techniques of Address Space Layout Randomization and Position Independent Executable are both related to mixing things up in the executable, so that nothing is in a predictable place. Also, since we are dealing with 64 bit executables, the amount of space available is huge and so trying to defeat this by guessing is infeasible.
Linux x64 Binary Exploitation with NX and ROP	No	2 Hours	In this lab, we will look at how to exploit a binary when NX is turned on. NX is a protection mechanism that prevents execution on the stack. This would defeat any exploits that require placing the shellcode on the stack and jumping control to it. The main way of dealing with a non executable stack is to use the program's own code against itself.
Linux x64 Binary Exploitation with Stack Canaries (Part 1)	No	2 Hours	In this lab, we will look at how stack canaries are used to prevent stack based buffer overflows and potential ways that they can be defeated. We will be using gdb with the gef plugin to examine the binary and help develop the exploit. We will then use python with pwntools to develop an exploit script.
Linux x64 Binary Exploitation with Stack Canaries (Part 2)	No	2 Hours	In this lab, we will continue our look at how stack canaries are used to prevent stack based buffer overflows and potential ways that they can be defeated. We will be using gdb with the gef plugin to examine the binary and help develop the exploit. We will then use python with pwntools to develop an exploit script. In this part, we will examine how arbitrary memory reads and writes can be used to defeat canaries.
Live Imaging with FTK Imager and Data Recovery with Autopsy	**YES**	2 Hours	Students will create a live image using FTK Imager and verify that the image was created successfully.
Live Imaging with FTK Imager Lite	No	1 Hour	Students will use FTK Imager Lite to create a forensic image of a Windows 8 workstation. After they create the image they will perform a hash check to ensure that the image that was created is the same as what is currently running on the live system.
LNX101 - Fail2Ban Setup and Analysis	No	1 Hour	In this lab, you will learn how to install, configure and test Fail2ban in virtualized environment.
LNX101 - File System Structure	**YES**	1 Hour	In this lab, you will learn the basic file system layout and structure in a typical Linux distribution. After learning about each command, feel free to test it out in the virtual machine provided to you.
LNX101 - OpenSSH Installation, Configuration, and Hardening	**YES**	1 Hour	In this lab, you will learn how to install, configure, harden and test an OpenSSH server.
LNX101 - Setting Up a Firewall With UFW and Firewalld	No	1 Hour	In this lab, you will learn how to use two common firewall management tools called UFW or Uncomplicated Firewall and Firewalld.
LNX101 - Telnet vs. SSH	No	1 Hour	In this lab, you will learn how to use telnet, an insecure protocol that sends its data over the network in an unencrypted form.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Log Analysis	**YES**	1 Hour	In this lab students will have the opportunity to review various log files associated with the Windows operating system. Upon completing this exercise, the will be able to configure systems to log events and analyze system events.
Log Correlation	**YES**	1 Hour	Students will use Splunk to ingest server logs and a physical access log to determine if a physical security event has occurred, and if so, who may be behind it.
Log Correlation & Analysis to Identify Potential IOC	**YES**	1 Hour	When defending networked digital systems, attention must be paid to the logging mechanisms set in place to detect suspicious behavior. In this lab, students will work with Splunk to help correlate server logs, system logs, and application logs in order to determine if an attacker was successful, and if so what happened and how they got in.
Log Event Reports	No	1 Hour	Students will use system logs to create a report.
MAC Analysis	**YES**	1 Hour	Students will use this lab to become familiar with locations of data on a MAC Image.
Man In the Middle Crypto Attack	No	1 Hour	Students will be placed in the middle of an encrypted chat session. They will be able to analyze the protocol, find the flaws, formulate an attack, and execute the attack.
Manage Users and Groups in Windows	No	2 Hours	In this lab students will use PowerShell and Local Users and Groups tool to manage user and group accounts. The students will create, modify, and delete local user accounts and local groups within PowerShell. They will also manage local user accounts and groups using the Local Users and Groups within the Computer Management Microsoft Management Console (MMC) tool.
Manual Vulnerability Assessment	**YES**	1 Hour	As part of the defense in depth model it is vitally important to keep tabs on the events occurring on individual devices/systems. In this lab, students will use nmap to conduct a manual service scan to discover any networked devices as well as the services those devices are running. Next, they will log into a Windows workstation to set up auditing for system services, and then enable the auditing of attempts (successes/failures) to use a specific program (Splunk). Finally, the students will validate that the new audit objects are successfully working by reviewing the Event Log for the Windows workstation host.
Manually Analyze Malicious PDF Documents	**YES**	1 Hour	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.
Manually Analyze Malicious PDF Documents 2	**YES**	1 Hour	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.
Manually Creating a Baseline with MD5Deep	**YES**	1 Hour	Students will create a baseline on a documents folder using md5deep. Students will then modify the folder and observe the changes made to that folder.
Memory Extraction and Analysis	**YES**	1 Hour	This is one of the labs for the Advanced Digital Media Forensics class.
Metadata Extraction Lab	**YES**	1 Hour	In this lab, students will understand what Metadata is and learn a tool to use to identify it.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
MITRE - Attack	No	1 Hour	Threat hunting is performed with the assumption that intruders already exist within the network. As preventative measures aren't always effective, threat hunting focuses on finding and removing existing threats. In this lab, we'll take a look at threat hunting techniques and their role in cyber defense.
MITRE - Defense	No	1 Hour	Threat intelligence is an important part of cyber defense that allows cybersecurity professionals to more accurately and strategically defend their network and respond to attacks. This lab will take a look at the threat intelligence lifecycle and its role in cyber defense.
Mobile Device Management - Android O/S	No	2 Hours	This lab familiarizes the student with Mobile Device Management Systems, specifically the Android enrollment process. By the end of the lab, the student will have the Knowledge, Skills, and ability to enroll devices into an MDM system.
Monitoring and Verifying Management Systems	**YES**	1 Hour	Students will analyze a MBSA Baseline report and compare it to current system configurations. Students will then make necessary system changes to machines and validate baseline using MBSA. Students will finally compare hash values to determine if any changes have been made to a system.
Monitoring for False Positives	**YES**	1 Hour	In this lab we will map a drive to a share on the network and then copy resources from a file server.
Monitoring Network Traffic	**YES**	1 Hour	In this lab we will replicate potentially malicious scans from the Internet against a corporate asset. Scans from the Internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the web logs.
Monitoring Network Traffic for Potential IOA/IOC	No	1 Hour	In this lab we will replicate potentially malicious scans from the Internet against a corporate asset. Scans from the Internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the web logs.
Nessus Scanning and Reporting	No	3 Hours	This exercise will introduce trainees to the advanced settings within the Nessus Vulnerability Scanner. Trainees will modify scan settings to perform different types of scans and to learn about the different functionalities Nessus provides. Trainees will then compare the results of a Nessus scan against the results of a NMAP scan against the same target and discuss the differences and similarities between the two tools. Lastly, trainees will use the “Export” feature to generate Nessus reports.
Nessus Setup and Config	No	3 Hours	This exercise will familiarize trainees with the Nessus Vulnerability Scanning tool. Trainees will be able to install and configure Nessus after completing this exercise.
Network Discovery	**YES**	2 Hours	The Network Discovery lab is designed to help students facilitate open source collection by teaching them how to use more intimate network discovery techniques.
Network Miner	**YES**	1 Hour	This lab exercise is designed to allow the trainee to become familiar with using Network Miner.
Network Segmentation (FW/DMZ/WAN/LAN)	**YES**	1 Hour	Create three distinct areas for this network, route traffic accordingly and lock down VPN access to the appropriate IP address.
Network Topology Generation	**YES**	1 Hour	Students will utilize Zenmap to generate a visual network topology.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Nexpose: Analysis & Reporting (Executive, High Risk and Recommendation Reporting)	No	1 Hour	In this lab students will use Rapid 7's Nexpose vulnerability scanner to identify, assess, and report on network based threats. The lab contains multiple virtual environments each having its own operating system, vulnerabilities and dependencies. The environmental conditions of this lab provide a robust simulation for real world blue team defense strategy.
Nexpose: Blue Team Remediation	No	3 Hours	The Nexpose BlueTeam remediation lab will teach students how to run the nexpose remediation report, analyze high risk machines and remediate critical threats.
Nexpose: Red Team Exploitation	No	1 Hour	The Nexpose red team exploitation lab exposes student to the impact of critical network threats from an attacker perspective.
Open and Close Ports on Windows 7	**YES**	1 Hour	In this lab, the student will kill some processes and close down some shares in response to a suspected threat. Student will then determine the potential adverse effects to the network based on service requirements.
Open Source Collection	**YES**	2 Hours	The Open Source Collection lab is designed to familiarize students with the advanced functionality of Google, default webpages used for web-servers, and the specifics of Google Hacking database. This allows the students to understand how open source information can be used for exploitation purposes.
Open Source Password Cracking	**YES**	1 Hour	Students will use John the Ripper and Cain and Abel to crack password protected files
Overview of Kibana	No	1 Hour	Students will become familiarized with data visualization using Kibana - one of the 3 tools included in Elastic's ELK stack, a trio of open-source applications that work together in order to meet a myriad of different monitoring and analytics needs.
PAM Lab	No	1 Hour	This lab exercise is designed to allow trainees to remotely access a virtual machine using SSH to create a user account and assign the user account permissions on the virtual machine.
Parse Files Out of Network Traffic	**YES**	1 Hour	This lab teach students how to extract various files from network traffic using Network Miner and Wireshark.
Participate in Attack Analysis Using Trusted Tool Set	**YES**	1 Hour	Students will participate in attack analysis/incident response, including root cause determination, to identify vulnerabilities exploited, vector/source and methods used (e.g., malware, denial of service). Students will then investigate and correlate system logs to identify missing patches, level of access obtained, unauthorized processes or programs.
Password Cracking with PRTK	**YES**	2 Hours	In this lab, students will learn how to use Access Data's Password Recovery ToolKit (PRTK) to crack various types of passwords.
Patch Installation and Validation Testing	**YES**	2 Hours	Students will identify if a vulnerability is present on two Windows systems and then move to remediate the vulnerability, if necessary.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Patching With WSUS	**YES**	2 Hours	Students will have access to a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 7 client. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the Open Vulnerability Assessment System (OpenVAS).
Penetration Tester Challenge	**YES**	1 Hour	The objective of this scenario is to deface the corporate web server. In order to accomplish this objective, you need to complete a series of tasks designed to test your ability to enumerate and identify potential system and network vulnerabilities, exploit systems and/or networks based on vulnerability discoveries, recover system user credentials, use recovered credentials to pivot onto other information systems in the network(s) and establish a connection to deface the corporate web server.
Performing an Initial Attack Analysis	**YES**	1 Hour	Students will use perform incident response on a compromised machine.
Performing Incident Response in a Windows Environment	**YES**	1 Hour	This next lab walks students through identifying a security incident, as well as handling and then responding to the incident.
Personal Security Products	**YES**	1 Hour	Anti-virus (AV) programs are software designed to detect and quarantine programs that are deemed malicious. These applications were originally designed to remove malware from infected computers. Over time, AV products evolved to protect against other threats such as keyloggers, worms, and malicious websites. In this lab you will install, configure and use anti-virus to help defend your system.
Phishing	**YES**	1 Hour	Students will send a phishing email using the Social Engineering Toolkit. Students will then impersonate a user clicking on the attachment to observe how dangerous they can be and generate a phishing awareness email to educate users of the dangers of clicking unknown links.
Physical Security	**YES**	1 Hour	In this lab you will simulate an attack involving physical access to a workstation. Phyiscal security is important because if an attacker, or you as a penetration tester, have physical access to a machine, it is very difficult to stop a determined effort to gain access to that machine.
Post Exploitation and Pivoting	No	2 Hours	In this lab, we expand on our initial coverage of Metasploit and we will look at what to do once the target is compromised.
Post Incident Service Restoration	No	1 Hour	In this lab, as part of the recovery process, the student will restore services to a host in a post-incident environment. Startup services, and firewall settings, will both need to be addressed.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Practical Malware Analysis Labs	No	1 Day, 16 Hours	NOTE: This lab requires the following textbook: "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig". MAL600 exposes students to the theoretical knowledge and hands-on techniques to reverse engineer malware that was designed to thwart the most common reverse engineering techniques. The students learn how to identify and analyze the presence of advanced packers, polymorphic malware, encrypted malware, and malicious code armored with anti-debugging and anti-reverse engineering techniques. Students gain a high-level understanding of complex malware analysis techniques and spend a significant amount of time solving hands-on challenges throughout the course. This course is for malware analysts, or aspiring analysts, who have already taken CYBRScore's MAL400 (Fundamentals of Malware Analysis) and MAL500 (Reverse Engineering Malware) courses. Those who have encountered malware analysis as part of incident response, research, or secure development and want to improve upon their knowledge and skills may also find this course beneficial. Students should have intermediate malware analysis skills, the ability to read and understand moderately complex high-level language code constructs in assembly, familiarity with Windows API, networking, and scripting, and finally, experience with IDA Pro, Olly, Immunity, or another similar application.
Preliminary Scanning	**YES**	1 Hour	Students will utilize Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as routers.
Preparing Target Media	**YES**	1 Hour	In this lab, students will prepare target media for imaging using dc3dd and Disk Wipe.
Protect Against Beaconing	**YES**	1 Hour	Students will take a PCAP indicating the presence of a beacon on the network and analyze it. The analysis will determine if there's activity that we can mitigate mitigation and then implement a Firewall block with logging to prevent future beaconing.
Python	No	2 Hours	The Python Tool Building lab is divided into two parts: Python Fundamentals and Python Tool Building. If you're new to Python, or have limited experience, please complete the exercises found in part one. The exercises will provide you with a primer on important Python fundamentals. If you have experience with Python, you may want to skip the first section, or simply refer to it during the labs. In part two, you will build several scanning/enumeration and exploitation scripts. These scripts will demonstrate the power and usefulness of Python when performing penetration tests and red team exercises. The scripts are meant to be fairly straightforward proof-of-concepts to get your started. You are highly encouraged to customize and extend the scripts to work beyond the scenarios provided.
Python Tool Building - Authenticated SQLi	No	2 Hours	In this lab, you will exploit a very simple SQL injection vulnerability, as an authenticated user, using a Python script. Prior to writing the script, we will walk through the steps necessary to perform the injection manually so that you have a proper understanding of the steps required to perform this task with Python.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Python Tool Building - Banner Grabber	No	2 Hours	In this lab, we will be writing a short Python script that performs a banner grab on several ports. While you will often be able to use tools such as netcat or telnet to perform banner grabs, it is useful to know how to write a quick script that you can deploy on an engagement should your traditional tool set be unavailable.
Python Tool Building - C2	No	2 Hours	In this lab, students are given a compromised machine on which they will place an agent. This agent will need to beacon out for instructions, execute commands, and push the data to a remote server.
Python Tool Building - Local File Inclusion	No	2 Hours	In this lab, there is an intentionally vulnerable file that has a local file inclusion vulnerability hosted on your machine. Students will write a script that checks for the availability of files outside of the web root.
QRADAR - Auditing Service Accounts and Generating SIEM Reports	No	2 Hours	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the pull method (where the logging device itself pulls the logs off target devices). This lab will deal with the most common method, pull method, used today in log aggregation, that is, ie. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.
QRadar - Centralized Monitoring	No	1 Hour	This lab will help the students understand common logs in linux and to configure a remote system to forward syslog events to a central location (QRadar).
QRADAR - Collecting Logs and Verifying Syslog Aggregation with pfSense	No	2 Hours	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the pull method (where the logging device itself pulls the logs off target devices). This lab will deal with the most common method, pull method, used today in log aggregation, that is, ie. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.
QRadar - IDS Setup and Configuration	No	1 Hour	Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection/Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snoby SEIM when they hit.
QRadar - Log Correlation & Analysis to Identify Potential IOC	No	1 Hour	When defending networked digital systems, attention must be paid to the logging mechanisms set in place to detect suspicious behavior. In this lab, students will work with QRadar to help correlate server logs, system logs, and application logs in order to determine if an attacker was successful, and if so what happened and how they got in.
QRadar - Log Correlation & Analysis to Identify Potential IOC with Custom Log Types	No	3 Hours	This lab will teach users how to use QRadar to correlate logs from varying sources, and create custom log types for unknown events.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
QRADAR - Setting Up SYSLOG Forwarding From a Windows System	No	2 Hours	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the pull method (where the logging device itself pulls the logs off target devices). This lab will deal with the most common method, pull method, used today in log aggregation, that is, ie. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.
QRadar - Snort Signatures, IDS Tuning, and Blocking	No	1 Hour	Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection/Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the QRadar SEIM when they hit.
Ransomware	No	1 Hour	Students will learn what ransomware is, observe how it works, and implement mitigation strategies to recover from a ransomware attack.
Recover from Browser-based Heap Spray Attack	No	1 Hour	After identifying a browser-based heap spray attack used against a corporate asset, students will learn about EMET and the role it plays in recovery from a variety of attack vectors.
Recover from Illegal Bitcoin Mining Incident	**YES**	1 Hour	Students will conduct recovery activities using Indicators of Compromise found on the victim computer and other network-related artifacts. Students will also conduct recovery operations by looking for evidence of reinfection, malicious network activity, and checking patch levels and hotfixes applied to the victim computer.
Recover from Incident	**YES**	2 Hours	This lab covers a variety of concepts, and exercises static and dynamic analysis skills related to malware identification and eradication. After identifying and analyzing a malicious executable in a test environment, use the information gained to recover from an incident, and remove the malicious file from the victim's computer.
Recover from SQL Injection Attack	**YES**	1 Hour	After identifying a SQL Injection attack, students will learn about parameterized queries in back-end web servers to minimize future SQLi attacks.
Recover from Web-Based Flashpack Incident	No	1 Hour	Students will recover a Windows 7 client infected by an unknown payload loaded after exposure to the FlashPack Exploit Kit. The recovery will encompass network traffic analysis to determine infection vector and payload delivery mechanisms as well as system-specific recovery procedures to restore the system to its original functionality.
Recovering Data and Data Integrity Checks	No	1 Hour	In this lab, the student will establish a baseline of two pre-defined files, delete those files, and subsequently restore them. After restoration, the student will perform an integrity validation on the recovered files.
Recovery From Inadequate Patching	No	2 Hours	Students will become familiar with procedures used backing up data, patching the system after a reported attack, checking the system for new vulnerabilities and then performing a rollback.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Registry Analysis	**YES**	3 Hours	In this lab, students will understand what type of information is contained within the Windows Registry as well as where to find the information.
Remove Trojan	No	1 Hour	In this lab, the student will execute a defined response plan to identify and remove a Trojan virus from a Windows environment using Windows Security Essentials.
Report Comparison and Evaluation	**YES**		Students will generate reports from Core Impact and from OpenVAS and compare the discrepancies between the two. Students will also identify the positive and negative qualities for both report types.
Report Writing for Presentation to Management	**YES**	1 Hour	In an earlier lab, students analyzed a suspected exploit (FlashPack Exploit Kit) on a corporate machine. In this lab they will find evidence of another FlashPack infection in using previously captured network traffic. In this scenario they will determine the details about how this attack was successful and will fill out a report with their findings. This report will then be used to brief the Management Team, as well as note the incident for future tracking purposes.
Respond to and Validate Alerts from Antivirus Software	No	1 Hour	Students will respond to and validate alerts from Antivirus software.
Reverse Engineering Malware	No	1 Day, 16 Hours	NOTE: This lab requires the following textbook: "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig". MAL500 builds upon our Fundamentals of Malware Analysis course and exposes students to the theoretical knowledge and hands-on techniques used to analyze malware of greater complexity. In Reverse Engineering Malware, students will learn how to reverse and dissect malicious Windows programs, debug user-mode and kernel-mode malware, as well as identify common malware functionality and hiding techniques. This course is for malware or aspiring-malware analysts who have already taken CYBRScore's MAL400 (Fundamentals of Malware Analysis) course, or for those who have encountered malware analysis as part of incident response, research, or secure development, and want to improve upon their knowledge and skills.
Rogue Device Identification and Blocking	**YES**	1 Hour	Students will scan a network and identify rogue devices. Students will then customize the firewall rules to ensure that any rogue devices are blocked from communicating with other systems on the network.
RootKit	No	1 Hour	This lab is designed to introduce the student to a Windows rootkit and to some tools and techniques used in discovery and removal of the rootkit. This experience should provide them with a basic understanding of rootkits and the challenges they pose during the removal process.
Scanning and Enumeration	**YES**	3 Hours	In this lab, you will practice scanning and enumeration using several popular tools, and learn how they can be used together to create a thorough and efficient workflow during the enumeration phase.
Scanning and Mapping Networks	**YES**	2 Hours	Students will use Zenmap to scan a network segment in order to create an updated network map and detail findings on the systems discovered. They will use the material they generated to help them discover if there have been any changes to the network after they compare it to a previously generated network map/scan.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Scanning From Windows	**YES**	1 Hour	Students will leverage Scalnline, a windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).
Scanning with Nmap	No	1 Hour	In this lab, you will perform several scans but, using Wireshark, you will be able to view the scan traffic to see what the tool is actually doing under the hood.
Searching for Indicators of Compromise	**YES**	1 Hour	If a company has a vulnerable Internet facing application, it can be exploited. An analyst should know how to identify attacks by artifacts that are present in the IDS as well as evidence on the compromised system.
Secure Coding (C++) - Lab 1: Race Conditions	No	1 Hour	In this lab, we will look at attacks on race conditions and then cover how to fix them.
Secure Coding (C++) - Lab 2: Data Validation	No	1 Hour	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.
Secure Coding (C++) - Lab 3: Authentication	No	1 Hour	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.
Secure Coding (C++) - Lab 4: Access Control	No	1 Hour	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.
Secure Coding (C++) - Lab 5: Cryptography	No	1 Hour	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.
Secure Coding (C++) - Lab 6: Error Handling	No	1 Hour	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.
Secure Coding (C++) - Lab 7: Static Analysis	No	1 Hour	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.
Secure Coding (C++) - Lab 8: Buffer Overflows	No	1 Hour	When too much data is placed into a buffer, it can overwrite adjacent memory values leading to remote code execution or system crashes. This lab will explore such vulnerabilities and how to fix them.
Secure Coding (Java) - Lab 1: Race Conditions	No	1 Hour	In this lab, we will look at attacks on race conditions and then cover how to fix them.
Secure Coding (Java) - Lab 2: Data Validation	No	1 Hour	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.
Secure Coding (Java) - Lab 3: Authentication	No	1 Hour	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.
Secure Coding (Java) - Lab 4: Access Control	No	1 Hour	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.
Secure Coding (Java) - Lab 5: Cryptography	No	1 Hour	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.
Secure Coding (Java) - Lab 6: Error Handling	No	1 Hour	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Secure Coding (Java) - Lab 7: Static Analysis	No	1 Hour	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.
Secure Coding (Java) - Lab 8: Insecure Deserialization	No	1 Hour	Many languages use object serialization for communication as it can greatly ease development. However, in some cases, actions can be taken automatically when objects are deserialized, if certain conditions are present. If the serialized object is ever exposed to and end user, that user can tamper with and modify the object, either causing unauthorized changes in variables, or, if those conditions are present, execution of unauthorized code. This issue has been the source of several major security breaches. In this lab, we will examine this problem, see how it can be exploited, and demonstrate best practices for securing your code against these types of attacks.
Secure Coding (Python) - Lab 1: Race Conditions	No	1 Hour	In this lab, we will look at attacks on race conditions and then cover how to fix them.
Secure Coding (Python) - Lab 2: Data Validation	No	1 Hour	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.
Secure Coding (Python) - Lab 3: Authentication	No	2 Hours	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.
Secure Coding (Python) - Lab 4: Access Control	No	1 Hour	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.
Secure Coding (Python) - Lab 5: Cryptography	No	2 Hours	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.
Secure Coding (Python) - Lab 6: Error Handling	No	1 Hour	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.
Secure Coding (Python) - Lab 7: Static Analysis	No	1 Hour	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.
Secure Coding (Python) - Lab 8: Pickles and Imports	No	1 Hour	In this lab, we will look at Python Pickles and the Python import system. We will be able to fix the issue relating to Pickles, and we will discuss how to mitigate the issues with imports.
Securing Linux - Advanced IPTables	No	1 Hour	In this lab, we will dive deeper into the host based firewall tool iptables. We covered basic packet filtering in a different lab, so in this lab, we will cover some of the more advanced features of iptables.
Securing Linux - App Armor	No	3 Hours	App Armor is a Mandatory Access Control (MAC) system similar in purpose to SELinux. App Armor is most commonly associated with the Ubuntu distribution. We covered what MAC is and how it differs from Discretionary Access Control (DAC) in the lab from this series on SELinux. In this lab, we will cover how App Armor works and how to configure it in a functional environment.
Securing Linux - Basic Restrictions	No	1 Hour	Linux has the ability to natively place restrictions of various kinds on the users and processes that they run. In this lab, we will explore those restrictions and see how they can be applied and to what end they can be used to lock down a system. We will also explore what limitations can be placed on the authentication process, which includes adding additional methods of authentication.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Securing Linux - Capabilities and ACLs	No	1 Hour	Many people don't realize that there is more to the Linux permission functionality than the basic user, group, and everyone permissions with read, write, and execute. In addition to basic permissions, there are also Capabilities and Access Control Lists. Capabilities are a way of delegating root permissions in tiny chunks. Access Control Lists allow finer grained control of permissions. Many of these features make use of extended attributes, which we will cover first.
Securing Linux - Centralized Authentication	No	3 Hours	FreeIPA is an open source, fully featured system for managing user accounts and accesses to hosts, that has a number of features that we will cover that make it very useful and easy to use. It also supports Kerberos, the cryptographic protocol for managing access used by AD and consequently allows it to be used in an AD environment, as well as supporting Linux-specific features like mapping system users to SELinux users. In this lab, we will explore basic setup and configuration and look into a few of the features that we can use to limit access.
Securing Linux - Encryption	No	1 Hour	One of the most important components of security is encryption. How can we protect data from being read or modified by unauthorized parties? Strong authentication and authorization can go a long way to helping, but at times our data will be out of our control and protecting it will be out of our hands. In times like that, strong encryption can help provide the assurances that we need. In this lab we will discuss tools and techniques for encrypting the data on your hard drive - that is, data at rest. This is especially important for laptops that might get stolen or desktops placed where untrusted people might be able to physically access them.
Securing Linux - Firewalls	No	1 Hour	Firewalls are an important part of limiting network traffic. Properly implemented firewalls can greatly limit the amount of damage an attacker can do by enforcing access control on the network interface. They can also be incredibly useful for regulating the amount of traffic or allowing certain network translations to occur that provide extra functionality.
Securing Linux - Monitoring with SecurityOnion	No	2 Hours	In this lab, we are going to introduce Zeek in the context of a SecurityOnion installation. We will look at its most basic features, how it can be configured, and how it can be customized through the writing of scripts.
Securing Linux - Network Intrusion Detection	No	1 Hour	In this lab we are going to look at Network Intrusion Detection. Network based intrusion detection systems examine network traffic and look for potentially malicious traffic.
Securing Linux - Physical Security	No	1 Hour	Oftentimes, physical access to a machine will allow an attacker to compromise it. It may have a screen lock that requires a password, but if the attacker can simply reboot, there are several methods that can allow compromise of the machine. We will look at a few of these methods in the context of Linux machines and implement some protections against them.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Securing Linux - Secure Remote Access	No	2 Hours	Many of the machines that we access we do remotely. This means that there needs to be a way to access the machine over the network. Depending on who needs to access it and from where, it may need to be visible and potentially accessible to people who should not have access. There is always a balance between accessibility and security. In this lab, we will cover two major ways of giving remote access - SSH and VPN.
Securing Linux - SELinux	No	2 Hours	SELinux is a system that allows you to define how various entities in the system are allowed to interact. At a very basic level, it checks each interaction in the system and determines if it is allowed. SELinux is installed by default on Red Hat and Red Hat based systems. We will be using Fedora as our main example in this lab. You can install SELinux on other distributions, which is done on the Debian system in this lab that will be used for certain examples.
Securing Linux for System Administrators	**YES**	1 Hour	Linux environments are ubiquitous in many different sectors, and securing these environments is as important as securing Windows environments. This lab walks you through implementing least-privilege and strong security practices in a Linux environment. Specifically, you will walk through ways to secure your Linux box, look at and fix common areas of privilege issues/abuses, and get introduced to SELinux and how it helps when implementing least-privilege.
Sensitive Information Identification	No	1 Hour	Students will utilize Data Loss Prevention (DLP) software to identify documents potentially containing sensitive information. They will parse through results and delineate false positives from documents containing legitimate sensitive information.
Setting up Filters and Queries in Kibana	No	1 Hour	Students will focus on using filters and queries in Kibana to find indicators of compromise within the network.
Setting Up SYSLOG Forwarding From a Windows System	**YES**	1 Hour	Students will learn how to conduct manual scanning against systems using command line tools such as Netcat then they will login to a discovered system and enable object access verify that auditing to the object is enabled.
Setting Up Zones in a Firewall	**YES**	1 Hour	Students will configure a pfSense Firewall to create/isolate various network segments.
SETUID	No	1 Hour	This lab exercise is designed to build upon the students understanding of user and file permissions by using the setuid flag.
Sinkholing C2 Traffic	No	1 Hour	You have a known C2 Domain that has infected your network. You will create a DNS record and sinkhole all requests to this domain. This will allow your analysts to identify which machines are in your environment and also protect your network by redirecting systems that attempt to contact this domain.
Snap Exploit	No	1 Hour	In January 2019, a local privilege escalation vulnerability was discovered in Ubuntu's snapd service. This lab will discuss the vulnerability and show how to exploit it. Snap is a package manager and software deployment platform created by Canonical. It is included in Ubuntu by default in all versions since 16.04. The fix is to upgrade your snapd version to 2.37.1 or higher.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Snorby Setup and Operation	**YES**	1 Hour	This lab exercise is designed to expose trainees to perform an initial setup for Security Onion and to configure and install Snort and Snorby.
SNORT Configuration and Operation Lab	**YES**	1 Hour	This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will create a custom user account and group to run Snort and create/test a custom rule.
Snort Signatures, IDS Tuning, and Blocking	**YES**	1 Hour	Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection/Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snoby SEIM when they hit.
Specialized Linux Port Scans	No	1 Hour	Students will leverage Hping3 to assess ports of various devices on the assigned network. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).
System Hardening	**YES**	1 Hour	A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this lab you will focus on some ways you can safeguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardening, strives to reduce vulnerabilities in order to protect a system against threats and attacks.
TCPDump	**YES**	1 Hour	This lab exercise is designed to allow the trainee become familiar with the basic command arguments and usage of TCPDump.
Threat Designation	**YES**	1 Hour	Students will conduct scans against a web server, a file share, a printer and a user's host device. The student will identify specific threats posed to the system. Students will then scan a network and identify potential points of ingress (open ports, etc) that could cause compromise to the system.
Tweaking Firewall Rules for Detection	**YES**	3 Hours	Students will use organizational firewall for monitoring, detecting and auditing traffic on the network. Students will then configure log traffic of interest forwarded to a syslog server.
Use EFS to Encrypt Files on NTFS Volumes	No	2 Hours	In this lab students will use File Explorer to encrypt files and folders through Encrypting File System (EFS), and then test the configuration by attempting to access an encrypted file as a different user. Finally, the students will cipher.exe command line tool to manage EFS file encryption.
Use pfTop to Analyze Network Traffic	**YES**	1 Hour	Students will use pfTop, a network traffic monitoring/statistics plugin used in pfSense, to analyze and monitor network traffic. They will walk through the steps of performing a detailed investigation to determine what type of traffic is occurring across the exercise network. Finally, with the use of use visualization tools they will be able to further analyze network traffic statistics and learn how visuals can quickly aide in the incident response process.
Using PowerShell to Analyze a System	No	1 Hour	Students will be using Power Shell to search for running processes, users and tasks on local and remote systems in the user environment.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Using Snort and Wireshark to Analyze Traffic	**YES**	1 Hour	In this lab we will replicate the need for Analysts to be able to analyze network traffic and detect suspicious activity. Tools like Wireshark and Snort can be utilized to read, capture, and analyze traffic.
Validate Indications of Compromise: Analysis of PE File	No	1 Hour	Malware authors frequently use certain functions, symbols and other tools as a way of building and obfuscating the true nature of their executables. As part of the Detect phase you should be able to detect evidence of and determine if an executable is malicious, and be able to provide information that can be used to create signatures to detect it in the future.
Verify Attributes of Identified SilentBanker Intrusion	**YES**	1 Hour	Students will verify attributes of the identified intrusion with existing internal and external intrusion, pattern and malware databases.
Verify Attributes of Intrusion Through Additional Analysis	**YES**	1 Hour	Students will validate potential intrusions identified by monitoring systems and perform additional analysis.
Verifying Hotfixes	No	1 Hour	Software patches repair bugs or vulnerabilities found in software programs. Patches are simply updates that fix a problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. In this lab, you will learn how to identify currently installed patches, manually install a hotfix and configure a work around.
Virtualization	No	1 Hour	This lab is designed to provide students with the experience of creating a simple virtual machine (VM) using VMware Player.
Vulnerability Analysis/Protection	**YES**	3 Hours	Students will use OpenVAS to do a vulnerability analysis. Students will then identify applicable vulnerabilities and protect their system(s) against them.
Vulnerability Identification and Remediation	**YES**	1 Hour	Learners will use Nmap and OpenVAS/Greenbone Vulnerability Scanner to confirm old vulnerable systems and to also discover new ones. They will perform a risk analysis of the findings and determine steps to be taken to mitigate the issues discovered. Finally, armed with a previously completed audit report as an example, they will fill out the necessary audit documentation to provide details on their findings and to add any suggested mitigations.
Vulnerability Proof of Concept and Remediation	**YES**	1 Hour	Students will identify if a vulnerability is present in the systems and remediate the vulnerability if necessary.
Vulnerability Scan Analysis	**YES**	1 Hour	Students will run a Core Impact or Nessus Scan and identify vulnerabilities. Students will then view the report and prioritize vulnerabilities according to risk.
Vulnerability Scanner Set-up and Configuration	**YES**	2 Hours	Students will setup and configure Core Impact in preparation of a vulnerability scan against an internal network.
Vulnerability Scanner Set-up and Configuration with OpenVAS	No	1 Hour	Students will utilize OpenVAS to identify hosts on a network and assess their vulnerabilities.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Web 201 - Lab 1: Recon Tools	**YES**	1 Hour	In this lab we are going to cover a number of recon tools that should be used in the beginning of any web application penetration test. These tools will give you a foundation on which to base the bulk of the test. The key to a successful web application test is knowing what the application consists of. These tools will help to give a more complete picture of this at the beginning.
Web 201 - Lab 2.1: Detecting and Exploiting Hard to Find SQL injections	No	1 Hour	In this lab, we will look at a few different examples of how our input could be processed or blocked. We will explore several different evasion techniques to achieve our goals.
Web 201 - Lab 2.2: Advanced Sqlmap	No	2 Hours	In this lab we will explore some more advanced features of the SQL injection tool sqlmap, that will enable us to use it to exploit more difficult SQL injection vulnerabilities. Cases in which the default usage of the tool will not be able to find or exploit the vulnerabilities.
Web 201 - Lab 2.3: Manual Blind SQL Injection	No	2 Hours	In this lab, we will cover how to exploit Blind SQL Injections manually. Typically, if you come across a blind SQL injection, you would use sqlmap to exfiltrate the data. However, sometimes you cannot get sqlmap to find the injection point, or you don't have it available on the system you are using, or perhaps it would be caught by an Intrusion Detection System and you need to be stealthy. In these cases, it is important to know how to exploit these issues manually.
Web 201 - Lab 2.4: NoSQL Injection	**YES**	1 Hour	In this lab, we will explore a few aspects of NoSQL injections. We will be using a Node.js application as an example, with a MongoDB backend.
Web 201 - Lab 3.1: Cross Site Scripting Filter Evasion	No	1 Hour	In this lab, we will explore a few different filters and how to evade them to display an alert box. We will then finish by implementing a cookie stealer in a place where filters are in place.
Web 201 - Lab 3.2: Exploiting Misconfigured CORS	No	1 Hour	In this lab we will compare and constrast default operation, secure configuration of CORS, and misconfigured CORS.
Web 201 - Lab 4: Advanced OS Command Injection	No	1 Hour	In the first part of this lab, we will explore some methods of evading the filters and still accomplishing the goal. In the second part of the lab, we will make the exploit even more difficult by leaving the filters in place as well as removing the output, making it a blind OS Command Injection.
Web 201 - Lab 5: Advanced Local File Inclusion	No	1 Hour	As an attacker, the two main goals in exploiting LFI are typically to expose secret or sensitive information or to cause arbitrary code to be executed, giving them remote command execution. For the former goal, you may want the source code for the application, which is made difficult in that the code is interpreted and executed and not directly displayed. For the latter goal, one of the main hurdles is getting your own code onto the server itself in order to be included by the application. We will deal with both of these issues in this lab.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Web 201 - Lab 6: Advanced CSRF	No	1 Hour	Cross Site Request Forgery (CSRF) is when an attacker can induce a victim to make a request to a site they are already authenticated to and cause them to make changes that they otherwise wouldn't want to do. For example, an attacker could cause the victim to change their password or their contact email without their knowledge. The best modern defence against CSRF is the anti-CSRF token, a random token generated per session that must be submitted with each request in order to ensure that the legitimate client is the source of the request. Since the attacker has no way of knowing this token, the attacker cannot cause the victim to submit it along with the change request. However, there is at least one case where that isn't true. That is, is the CSRF protected site also has a Cross Site Scripting vulnerability on a page that contains the token. An attacker may be able to leverage the XSS to leak the CSRF token, at which point the CSRF attack can be carried out.
Web 201 - Lab 7.1: XXE to Obtain Arbitrary Files	No	1 Hour	In this lab, we will explore the basic limitations of XXE and techniques that can be used in a PHP web application to overcome them.
Web 201 - Lab 7.2: Out of Band XXE Attacks	No	1 Hour	Sometimes there is an XML External Entity vulnerability, but exploiting it doesn't send any data back within the web application. If this is the case, it not only may be hard to detect that the issue exists, but it will also be difficult to exploit the issue.
Web 201 - Lab 8: Server Side Request Forgery	No	1 Hour	In this example we will be faced with a web application that will simply open whatever resource you specify, with increasingly strict restrictions. However, in a real application, this issue will likely be a bit harder to find. It might surface in an application that is acting as a proxy for some resource or it might simply be retrieving resources from a private network. In any case, some of the restrictions that we will explore may be natural restrictions based on how the application is implemented, or may be steps taken to secure the functionality.
Web 201 - Lab 9: Insecure Deserialization in Python and Java	No	1 Hour	Insecure Deserialization occurs when the web application takes a serialized object, that has been exposed to the user and possibly tampered with, and converts it back into an object. Several things can happen when a web application deserializes content that comes from an end user. First, if the object contains any information related to security, authorization level, or authentication information, the user can change that information and potentially elevate their privilege level. Second, depending on the system being used and the way in which objects are being deserialized, it may enable remode code execution. We will explore both of these possibilties in this lab, in the context of Python and Java
WEB241: Hardening PHP Web Apps - Broken Access Control	**YES**	1 Hour	This lab teaches methods to deploy basic access control in a web application written in PHP.
WEB241: Hardening PHP Web Apps - Broken Authentication	**YES**	1 Hour	This lab teaches methods to secure the authentication methods in a web application written in PHP.
WEB241: Hardening PHP Web Apps - Cross Site Scripting	No	1 Hour	This lab teaches methods to secure web applications written in PHP against XSS attacks.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
WEB241: Hardening PHP Web Apps - CSRF	**YES**	1 Hour	This lab teaches methods to secure web applications written in PHP against Cross Site Request Forgery attacks.
WEB241: Hardening PHP Web Apps - File Uploads	No	1 Hour	This lab teaches methods to secure web applications written in PHP with respect to file upload capabilities.
WEB241: Hardening PHP Web Apps - OS Command Injection	**YES**	1 Hour	This lab teaches methods to secure a web application written in PHP against OS Command Injection attacks.
WEB241: Hardening PHP Web Apps - Password Hashing	**YES**	1 Hour	This lab teaches how to properly use password hashing in a PHP web application.
WEB241: Hardening PHP Web Apps - Path Traversal and LFI	**YES**	1 Hour	This lab teaches methods to prevent Path Traversal and Local File Inclusion in a web application written in PHP.
WEB241: Hardening PHP Web Apps - PHP Configuration	No	1 Hour	This lab teaches methods to secure the PHP configuration for web applications written in PHP.
WEB241: Hardening PHP Web Apps - Secure Deserialization	No	1 Hour	This lab teaches methods to secure web applications written in PHP against Insecure Deserialization attacks.
WEB241: Hardening PHP Web Apps - Sensitive Data Exposure	No	1 Hour	This lab teaches how to prevent sensitive data exposure in a PHP web application.
WEB241: Hardening PHP Web Apps - SQL Injection	No	1 Hour	This lab teaches methods to secure a web application written in PHP against SQL Injection attacks.
WEB241: Hardening PHP Web Apps - Two Factor Authentication	No	1 Hour	This lab teaches how to deploy Google Authenticator in a PHP web application in order to deploy Two Factor Authentication.
WEB241: Hardening PHP Web Apps - XXE	No	1 Hour	This lab teaches methods to secure a web application written in PHP against XXE attacks.
WebApp Attack PCAP Analysis	**YES**	1 Hour	In this lab you will analyze a capture file of a web application attack in order to identify the attack vector and deduce the vulnerability the attack exploited.
Whitelist IP Address from IDS Alerts	No	1 Hour	Students will whitelist the approved scanning device so that no security alerts are generated from the host.
Whitelisting & Suspicious File Verification	**YES**	1 Hour	Students will become familiar with procedures used in the validation of suspicious files. During the course of the lab the student will generate a system-level baseline using a command line file hash tool, followed by checking new/unknown files against whitelists and online tools.
Windows Deployment Services	**YES**	1 Hour	As an incident responder, it's important to understand how to create baseline Windows templates. You will learn how Windows Deployment Services(WDS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WDS.
Windows Event Log Manipulation via Windows Event Viewer	No	1 Hour	In this lab you will use Windows Event Viewer to view and filter the security event log on a Windows 7 client computer specifically for account logons.
Windows Exploitation	**YES**	3 Hours	In this lab, you will learn techniques necessary to scan Windows machines for vulnerabilites and exploit a vulnerability to gain control of the victim machine. Note that this lab is highly guided step by step; in a real world penetration test, each of these steps will likely require significant trial-and-error.

LAB NAME	SCORED	DURATION	LAB DESCRIPTION
Windows Rootkits With Python	No	2 Hours	In this lab, we will use the Pywin32 extensions and the Deviare library to hook into functions and interact with the internal data structures. The Deviare library is a bit limited in terms of it capabilities as a rootkit, mainly since that is not what it was designed to do. However, it will be enough for our purposes and will enable us to more simply create a rootkit that uses a covert channel to exfiltrate data.
Windows System Hardening	**YES**	1 Hour	A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this lab you will focus on some ways you can safeguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardening, strives to reduce vulnerabilities in order to protect a system against threats and attacks.
Wireshark	**YES**	1 Hour	This lab exercise is designed to allow the trainee become familiar with the use of Wireshark.
x86 Buffer Overflows - Part 1	No	3 Hours	In this lab, students will write their own vulnerable program in C, debug the program while performing a buffer overflow, and control execution flow to jump to a function in the code that is not normally called.
x86 Buffer Overflows - Part 2	No	3 Hours	In this lab, you will fuzz and exploit vulnserver.exe, generate shellcode with msfvenom, and develop a working exploit locally that will then be used to exploit the service running remotely on another system.