COURSE TITLE	COURSE DESCRIPTION	LEARNING OBJECTIVE	PREREQUISITES	AVAILABILITY

cyrin CYBER RANGE

LEVEL 1 LABS

COURSE TITLE	COURSE DESCRIPTION	LEARNING OBJECTIVE	PREREQUISITES	AVAILABILITY
Introductory IDS Configuration with Snort	Students learn how to configure and run the widely-used, free OSSEC Host Intrusion Detection System (HIDS). During the exercise, students will learn how to check for rootkits using OSSEC, how to verify file integrity, how to set up passive and active responses, and more. Host intrusion detection is critical to maintaining a secure system, and is required by HIPAA and PCI regulations, both of which OSSEC can help you meet.	Students learn how to configure and run the widely-used, free OSSEC Host Intrusion Detection System (HIDS).	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available
Intrusion Detection using Zeek (formerly Bro)	Students learn how to deploy, configure and customize a Zeek Network Intrusion Detection System (NIDS). They will customize Zeek to generate enterprise specific logs and to send email notifications of events of interest. They will also create a simple Zeek plugin, using the Zeek scripting language to detect and block brute force ssh login attempts.	Students learn how to deploy, configure and customize a Zeek Network Intrusion Detection System (NIDS).	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available
Firewall Configuration with pfSense	Students will learn to set up firewall rules using the pfSense firewall and to configure a pfSense firewall using its Web-based user interface. Students will also learn to read and understand firewall logs.	Students will set up firewall rules that apply at certain times of the day; rules that allow or block access to certain hosts and ports; rules that block access from certain networks including bogons, and rules that apply when conditions (such as a certain number of failed login attempts) are detected.	Familiarity with the UNIX command line and knowledge of basic networking concepts (TCP/IP, DNS, etc).	Currently Available
Firewall Configuration with Iptables	Students will configure a network firewall using the standard Linux iptables module. The exercise will include both ingress and egress filtering, stateful packet inspection, and best practices. More advanced techniques such as port knocking will also be introduced. Evaluation will include network probes from both inside and outside the firewall to ensure proper rules are configured.	Students will configure a network firewall using the standard Linux iptables module.	Familiarity with the Unix/Linux command line Basic networking concepts (TCP/IP, DNS, etc.) Basic network routing concepts (firewalls, subnets, etc.).	Currently Available
Firewall Configuration with VyOS	Students will configure a network firewall using the VyOS router appliance, which mimics physical router hardware. The exercise will include both ingress and egress filtering, stateful packet inspection, and best practices. Students will set up a partitioned network and a DMZ area to isolate specific enterprise services, such as an e-mail server. Evaluation will include network probes from both inside and outside the firewall to ensure proper rules are configured.	Students will configure a network firewall using the VyOS router appliance, which mimics physical router hardware.	Comfort working with command-line environments. Basic networkingconcepts (TCP/IP, DNS, etc.)Basic network routing concepts (firewalls, subnets, etc.).	Currently Available

VPN Server Configuration with Open VPN	Students will learn to configure and set up an OpenVPN server. OpenVPN is an open-source virtual private network (VPN) solution. VPNs extend a private network over a public network, allowing users to send and receive data over the public networks as if they are directly connected to the private network. Students will learn to set up a Certificate Authority to create the keys and certificates needed to (1) authenticate users (VPN clients) and the VPN server and, (2) encrypt communication between the two. They will also learn how to revoke client certificates	Students will learn to configure and set up an OpenVPN server.	Basic knowledge of public key infrastructures and certificates Familiarity with the Unix/Linux command line.	Currently Available
Host Intrusion Detection System (IDS) Setup with OSSEC	Students will learn how to configure an Intrusion Detection System (IDS) to examine traffic to/from a firewall. The popular Snort® IDS will be used in this exercise. The exercise will include both harmless background traffic and potentially-malicious traffic to be detected by Snort.	Students will configure an Intrustion Detection System to examine traffic to/from a firewall.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available
Using Active Directory to Manage Domain User Accounts	Students learn to use the Windows Active Directory service to create and manage domain user accounts. They also learn to set up security policies and assign these policies to users and organizational units.	Students learn to use the Windows Active Directory service to create and manage domain user accounts.	Some familiarity with the Windows desktop.	Currently Available
SSH Server Configuration	Students learn the proper setup of the OpenSSH remote administration tool including security-relevant settings. During the exercise, students will learn best practices such as host filtering, public-key or Kerberos authentication, and PAM integration.	Students learn the proper setup of the OpenSSH remote administration tool, including a security-relevant setting.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available
Identifying Live Machines and Services on an Unknown Network	Students will use tools such as nmap, unicornscan, and fping to identify systems on a local network, including both Unix and Windows targets. Students will identify the operating systems these systems are running, as well as the types of network services they are providing.	Students will use tools such as nmap, unicornscan, and fping to identify systems on a local network, including both Unix and Windows targets.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available
Service Identification I	Students will use multiple tools to identify services including software package and version information running on unknown systems. Network services to be targeted will include those running on non-standard ports or behind firewall rules.	Students will use multiple tools to identify services including software package and version information running on unknown systems.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).Basic operating system security concepts.	Currently Available
Service Identification II	Students will build on the Service Identification I exercise to use service-specific information-gathering tools. Students will gather vendor, software, and version information, as well as any configuration information available remotely. Students will then use scripting tools to automate this process.	Students will build on the Service Identification I exercise to use service-specific information-gathering tools.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).Basic web application knowledge (HTTP, URL parameters, etc.).	Currently Available
Log Analysis with RSYSLOG	This lab teaches students to setup and configure a central RSYSLOG server that will receive and store logs from FreeBSD, Linux and Windows clients. Students will learn to configure log forwarding on the clients, and log rotation and filtering on the server. They will also learn to use Logwatch to analyze logs and fail2ban to automatically respond to suspicious activity found in the logs.	This lab teaches students to setup and configure a central RSYSLOG server that will receive and store logs from FreeBSD, Linux and Windows clients.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).Basic web application knowledge (HTTP, URL parameters, etc.).	Currently Available

Log Analytics with Splunk	In this lab the student will learn how to configure and securely run the Splunk Enterprise security information collection and analysis platform. The objective of the lab is to deploy multiple instances of Splunk data forwarders through a deployment server and analyze the logs received from the servers. The student will write custom scripts to generate logs, create both visual and textual reports, organize these reports into a single dashboard, and learn to recognize malicious activity.	In this lab the student will learn how to configure and securely run the Splunk Enterprise security information collection and analysis platform.	Ability to use a command line editor (vi, vim, nano, or emacs).Familiarity with the Linux and Windows environment and command line tools.Basic understanding of shell scripting in BASH and PowerShell.Intermediate understanding of networking concepts and services (TCP/IP, SSH, ...).	Currently Available	
Log Analytics with Elastic Stack	Elastic Stack is a group of services designed to take data from almost any type of source and in almost any type of format to search, analyze and visualize that data in real time. In this lab Elastic Stack will be used for log analytics. Students will learn to set up and run the Elasticsearch, Logstash and Kibana components of Elastic Stack. Multiple computers in a small network will forward their logs to a central server where they will be processed by Elastic Stack. Students will use Kibana to view logs, filter them and set up dashboards. Information in the logs will be used to identify and block an on-going attack.	Students will learn to set up and run the Elasticsearch, Logstash and Kibana components of Elastic Stack.	Basics of Linux/Unix shell commands;some familiarity with the concepts of sudo and ssh.	Currently Available	
Introduction to Metasploit	Students will gain experience with the widely-used open source Metasploit® framework for exploiting vulnerable software. The exercise includes launching attacks against well-known, unpatched software on multiple platforms—including examples of unauthorized administrator access on a remote system. By seeing the tools available to potential attackers, students will gain a greater appreciation for the need to keep software up-to-date and securely configured.	Students will gain experience with the widely-used open source Metasploit® framework for exploiting vulnerable software.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).	Currently Available	
Vulnerability Scanning with OpenVAS	Students will use the free OpenVAS web tool suite to identify vulnerabilities in services available on an unknown network. The network will include several targets with known-vulnerable software versions and/or configurations.	Students will use the free OpenVAS web tool suite to identify vulnerabilities in services available on an unknown network. The network will include several targets with known-vulnerable software versions and/or configurations.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).Basic operating system security concepts.	Currently Available	
Automating Security Analysis with SPARTA	Students will build on the results of labs in the Web Application Security Analysis and Network Monitoring categories by using the SPARTA network infrastructure penetration testing tool, a graphical application that automates many common vulnerability assessment tasks. Students will use SPARTA within a graphical Kali Linux environment, scanning multiple unknown target systems and exploring found weaknesses.	Students will build on the results of labs in the Web Application Security Analysis and Network Monitoring categories by using the SPARTA network infrastructure penetration testing tool.	Familiarity with the Unix/Linux command line.Basic Networking Concepts(TCP/IP, DNS, etc.).Basic web application knowledge (HTTP, URL parameters, etc.).	Currently Available	

Secure Configuration of the Apache Web Server	Students will learn how to set up a web server securely by configuring the commonly-used Apache HTTP Server® on a Linux system. Security options will be explored, including location/directory restrictions, permissions, authentication, and SSL configuration	Students will learn how to set up a web server securely by configuring the commonly-used Apache HTTP Server® on a Linux system.	Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Secure SSL Configuration in Apache	Students will build on the basic Apache configuration exercise to configure Secure Sockets Layer (SSL) encryption for the Apache HTTP Server®. Students will learn and implement best security practices and strong cryptography guarantees while avoiding vulnerabilities such as Heartbleed.	Students will build on the basic Apache configuration exercise to configure Secure Sockets Layer (SSL) encryption for the Apache HTTP Server	Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Web Application Security Analysis Using OWASP-ZAP	Students will use the OWASP program's ZAP tool suite from within Kali Linux to scan multiple web services and document vulnerabilities. Students will see ZAP in action on a vulnerable web site where entire database tables are available to potential attackers.	Students will use the OWASP program's ZAP tool suite from within Kali Linux to scan multiple web services and document vulnerabilities.	Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Web Application Security Analysis Using Nikto	Students will use the Nikto tool to test web services over the network and document vulnerabilities. Students will then use network packet capture tools such as Wireshark to verify their understanding of the vulnerabilities and testing procedures.	Students will use the Nikto tool to test web services over the network and document vulnerabilities.	Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Web Application Security Analysis Using Vega	Students will use the Vega scanning tool, within a graphical Kali Linux environment, to test web services over the network and document vulnerabilities. Students will then use network packet capture tools such as Wireshark to verify their understanding of the vulnerabilities and testing procedures.	Students will use the Vega scanning tool, within a graphical Kali Linux environment, to test web services over the network and document vulnerabilities.	Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Web Application Security Analysis Using BurpSuite	BurpSuite is an industry standard suite of tools used by information security professionals for testing Web application security. Its tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Students learn to use Burp tools to find security vulnerabilities in a web application. They will discover the application is vulnerable to cross-site scripting (XSS) attacks and will learn how to exploit the vulnerability to steal user credentials.	Students learn to use Burp tools to find security vulnerabilities in a web application. They will discover the application is vulnerable to cross-site scripting (XSS) attacks and will learn how to exploit the vulnerability to steal user credentials.	Basic web application knowledge (HTTP, URL parameters, etc.).	Currently Available
Detecting and Exploiting SQL Injection Vulnerabilities	Students will learn how to detect and exploit SQL injection vulnerabilities. By using several SQL injections techniques students will gather information about a remote database such as Operating System, database type, table names and their content. Students will then use sqlmap, a tool for SQL injection, to automate this process.	Students will learn how to detect and exploit SQL injection vulnerabilities.	Familiarity with the Unix/Linux command line Basic knowledge of SQL queries.	Currently Available

Website Reconnaissance	Information stored in the meta-data fields of files such as image files can provide valuable information for an incident investigation. Students will learn to use tools such as FOCA and exif to view and use this "hidden" information.	Students will use tools such as FOCA and wget to find and bulk download documents from a website. They will examine the metadata in these documents using the FOCA and exif tools to uncover information that the website would not have wished to make available publicly.	Basic knowledge of networking concepts (client-server architecture, routing, etc.) and the command-line.	Currently Available
DoS Attacks and Defenses	This lab teaches three different Denial of Service attacks and techniques to mitigate them: A TCP SYN Flood attack that exploits a weakness in the design of the TCP transport protocol, A slow HTTP attack called Slowloris that takes advantage of how HTTP servers work, A DNS amplification attack that exploits misconfigured DNS servers, of which there are plenty on the Internet.	This lab teaches students three different Denial of Service attacks and techniques to mitigate them.	Familiarity with the Unix/Linux command line. Basic web application knowledge (HTTP, URL parameters, etc.) Basic networking concepts (TCP/IP, DNS, etc.).	Currently Available
Handling Potential Malware	Students will learn to use the Cuckoo sandbox to determine if an executable or document is potential malware. If the executable is packed (compressed), they will learn to use a debugger to unpack it.	Students will learn to use the Cuckoo sandbox to determine if an executable or document is potential malware.	Basic knowledge of computer architecture and assembly language.	Currently Available
Introduction to P2P Forensics	Introduces students to the process of investigating usage of peer-to-peer (P2P) file sharing services for trading illicit content. Students learn what artifacts of P2P file sharing usage are left on a suspect's hard drive, as well as how to extract forensically-relevant information from the raw data. Students then use Architecture Technology Corporation's P2P Marshal™ software in a hands-on practical, gathering evidence from provided forensic disk images using Microsoft Windows®. A copy of the P2P Marshal software is available free of charge to anyone enrolled in this course.	This lab introduces students to the process of investigating usage of peer-to-peer (P2P) file sharing services for trading illicit content.	Basic cyber forensics knowledge and best practices are recommended.	Currently Available
Introductory File System Forensics	Disk-based analysis is the cornerstone of cyber forensics, whether it be to track what a suspect was doing or simply to recover accidentally deleted files. This lab introduces students to the process of imaging and forensically analyzing disks, including finding artifacts such as deleted files. The free Autopsy® forensic browser will be used in addition to command-line programs from the open-source Sleuth Kit® tool set.	This lab introduces students to the process of imaging and forensically analyzing disks, including finding artifacts such as deleted files.	In order to get the most out of this lab, you should be comfortable with cyber forensics best practices (chain of evidence, etc.) and be comfortable with a Linux/Unix command line.	Currently Available
Live Forensics Using GRR	GRR Rapid Response is an open source live forensics tool originally created by Google. GRR allows an investigator to collect data about running systems on a network, anywhere from one system to thousands. In this lab, students will perform live remote forensic investigations against running systems. Without having to take the systems offline for imaging, students will examine running processes and network connections, files and disk artifacts, and registry keys across multiple target machines in a forensically-sound manner.	In this lab students will perform live remote forensic investigations against running systems.	You should have a basic familiarity with computer forensics processes and tools in order to get the most out of this lab.	Currently Available

Introduction to Memory Analysis with Volatility	Analyzing a suspect system "live", before disconnecting it and imaging the disks, often yields valuable forensic evidence. Further, it can help you determine whether a crime has been committed or whether the system contains evidence, thereby avoiding time-consuming examination of irrelevant machines. The Volatility® framework is the dominant open-source memory analysis framework, examining RAM snapshots from a large variety of operating systems in multiple formats. This lab introduces students to the process of capturing a live RAM image and analyzing it using Volatility. Students will learn about several Volatility plugins for analyzing a Windows memory image, then analyze actual RAM images, including one with active malware, and view the results.	This lab introduces students to the process of capturing a live RAM image and analyzing it using Volatility. Students will learn about several Volatility plugins for analyzing a Windows memory image, then analyze actual RAM images, including one with active malware, and view the results.	In order to get the most out of this lab, you should be familiar with cyber forensics best practices (chain of evidence, etc.) and be comfortable with a Linux/Unix command line.	Currently Available
Introduction to Memory Analysis with Rekall	Analyzing a suspect system "live", before disconnecting it and imaging the disks, often yields valuable forensic evidence. Further, it can help you determine whether a crime has been committed at all, or whether the system contains evidence at all, thereby avoiding time-consuming examination of irrelevant machines. Rekall is an advanced, open-source memory capture and analysis framework that has expanded to include a variety of live incident response tools. This lab introduces students to the Rekall framework, both for extracting evidence from memory images and for analyzing the current live state of the system. Students will learn about several Rekall tools, both on the command line and via the interactive console, for analyzing memory images. Students will then analyze several images of Windows systems with in-memory malware.	Students will learn about several Rekall tools both on the command line and via the interactive console for analyzing memory images. Students will then analyze several images of Windows systems with in-memory malware.	In order to get the most out of this lab, you should be familiar with cyber forensics best practices (chain of evidence, etc.) and be comfortable with a Linux/Unix command line. An understanding of operating systems concepts, such as processes and network connections, is also required.	Currently Available
Advanced P2P Forensics	This course builds on the Introduction to P2P Forensics in order to provide students with a deeper understanding of how to extract evidence from a suspect's hard drive. Students learn detailed file formats used by popular P2P software and methods for extracting information by hand. The course concludes with a hands-on practical using Architecture Technology Corporation's P2P Marshal™ and provided forensic disk images using Microsoft Windows®. A copy of the P2P Marshal software is available free of charge to anyone enrolled in this course.	Students learn detailed file formats used by popular P2P software and methods for extracting information by hand.	You should complete the Introduction to P2P Forensics course first in order to get the most out of this exercise.	Currently Available
eMule P2P Forensics	This course provides a deep dive into the eMule peer-to-peer file sharing system and client software. Students will learn how eMule stores forensically-relevant data on disk. The course concludes with a hands-on practical using Architecture Technology Corporation's P2P Marshal™ and provided forensic disk images using Microsoft Windows®. A copy of the P2P Marshal software is available free of charge to anvone enrolled in this course.	Students will learn how eMule stores forensically-relevant data on disk.	You should complete the Introduction to P2P Forensics course first in order to get the most of this exercise. The Advanced P2P Forensics course is recommended as well.	Currently Available
				COMING IN 2020
Protocol Analysis I: Wireshark Basics	This course is a comprehensive process to evaluate normal and abnormal traffic on the network. It will include evaluation of conversations on the network and components of a variety of traffic, including different attacks and the artifacts that identify the attacks.	Students will learn how to identify normal network traffic and learn how to distinguish characteristics of a variety of attacks at the network level.	Networking knowledge and an understanding of how IP addresses are assigned and used.	

Protocol Analysis II: Advanced Wireshark	This course is a continuation of the analysis of network traffic. It includes web attacks, application attacks and advanced sophisticated attacks that use remote access trojans and web shell.	Students will review attacks for web applications as well as the characteristics of advanced and sophisticated attacks to include communications of web shells.	Completion of the Protocol Analysis One or equivalent. Characteristics of attacks at the packet level.	
Protocol Analysis III: Extracting Data from Network Traffic	This course will continue with exploration of low-level analysis to include the discovery of the artifacts of the different types of attacks at the lowest packet level. This includes searches using offsets, identifying nation state types of attacks and complex filters and queries to extract attack data.	Students will perform low-level traffic analysis of network traffic and learn how to extract data from the raw packets using offsets and complex filters and queries.	Completion of the Protocol Analysis Two or equivalent. Characteristics of attacks at the packet level.	
Secure DNS Configuration using Bind	Learn about split-horizon DNS and how to set one up. An organization with a split-horizon DNS has a public-facing DNS that resolves names for public-facing services. A second internal DNS is accessible on a private network and is used for resolving services internal to the organization. This lab shows how to set up two BIND nameservers for public and private name resolution.	Students will learn to set up a public facing DNS and an internal DNS for an organization. Students will set up two DNS zones and verify the policies set up for each zone.	Familiarity with the UNIX command line and knowledge of basic networking concepts (TCP/IP, DNS, etc).	

CYBER SECURITY SKILLS FOUNDATION COURSES

COURSE TITLE	COURSE DESCRIPTION	LEARNING OBJECTIVE	PREREQUISITES	AVAILABILITY
				COMING IN 2020
Cyber Skills Foundation	Each course will include power point instructional steps by module with the insertion of 10-15 CYRIN labs included in each course.	Students will learn the essential skills to build a solid security foundation. They will examine in detail the traffic that traverses the network at the packet and binary level. They will build solid knowledge on the lowest layers of the network.	Basic network knowledge.	
Essential Defense Tactics	Each course will include power point instructional steps by module with the insertion of 10-15 CYRIN labs included in each course.	Students will learn the foundation of security and defending architectures from attack. They will look at the concept of “thinking like a hacker” to learn techniques to defend from the types of attacks that are commonly conducted against the IT corporate networks as well as industrial control networks.	Basic network knowledge.	
Advanced Cyber Defense	Each course will include power point instructional steps by module with the insertion of 10-15 CYRIN labs included in each course.	Students will be evaluating advanced hacking methods of defense fortification bringing them closer to establishing perfect security best practices and methodologies they can apply to secure environments. This course provides segmentation and isolation to reduce the effectiveness of the advanced persistent threats.	Completion of course Essential Defense Tactics or equivalent knowledge.	

LEVEL 2 EXERCISES

COURSE TITLE	COURSE DESCRIPTION	LEARNING OBJECTIVE	PREREQUISITES	AVAILABILITY
Capture the Flag Scenario I	This exercise is designed to have students hone their skills and see how an attacker would exploit configuration weaknesses. This Capture the Flag (CTF) scenario lets students see first-hand an attacker's strategies for compromising their systems. It also asks the question - Can you gain total control over a target system solely via a web application?	The student or teams must capture three "flag" files from an unknown server. The difficulty increases with each one.	Familiarity with the UNIX command line and networking concepts, knowledge of web application vulnerabilities (e.g., SQL injection).	Currently Available
Capture the Flag Scenario II	Students build on their skills from the first CTF scenario with a new web server setup; which asks the question - can someone gain root access on this box? It allows students to hone their skills and see how an attacker would exploit configuration weaknesses. This Capture the Flag (CTF) scenario lets students see first-hand an attacker's strategies for compromising their systems. It also looks at whether you can gain total control over a target system solely via a web application.	The student or teams must capture three "keys" in this scenario, indicating increasing levels of access to the target. The difficulty increases with each one.	Familiarity with the UNIX command line and basic networking concepts (TCP/IP, DNS, etc), knowledge of web application vulnerabilities (e.g., SQL injection).	Currently Available
Conduct a Data Leak Investigation	In this scenario the student is a security officer for a shipping company whose trucks have been hijacked repeatedly by a criminal organization. Company executives suspect someone within the company is leaking truck route information to the criminals. Students are tasked with finding who is leaking the information, how and to whom.This investigation will be performed on an operational network i.e., unlike a forensics investigation students will not be working on disk images from computers on the network.	This exercise tests the students ability and skills at conducting an investigation into a data leak from a corporate network.	Knowledge of computer forensics concepts and tools, as well as centralized logging configuration and analysis.	Currently Available
				COMING IN 2020
Packet Capture Analysis and Manipulation	This exercise reviews the advanced filtering capabilities in Wireshark as well as mastering low-level packet analysis and advanced concepts of PCAP analysis with Wireshark and PCAP specific tools.	Students will be provided a review of the TCP/IP protocol and an introduction to custom packet creation and modification that is often used for obfuscation.	Completion of Protocol Analysis course or equivalent knowledge.	
Intrusion Analysis of Network Traffic	Students will receive a collection of PCAP files based on the latest malware that has been seen in the wild. They will have to analyze attack techniques of tunnelling and obfuscation. Assessment will include using static and dynamic PCAP challenges .	Students will learn a process and methodology for analysis of malware traffic by receiving a group of malware capture files.	Completion of PCAP One or equivalent knowledge.	
Advanced Analysis of Malicous Network Traffic	In this exercise, egress techniques will be used for both the spread and the command and control of the latest threats. Analysis of the techniques includes using the allowed outbound ports and protocols. Tools that can assist with the analysis of malware infections and command and control will be incorporated into this exercise.	Students will learn methods of Command and Control that are used by the latest malware threats.	Completion of PCAP One and Two or equivalent knowledge.	

Red team / blue team	Students will join the lab as a member of a "blue" team defending a network or a "red" team attempting to get to sensitive information on the network. As a red team member students will exercise their skills developed on the CYRIN labs in the Vulnerability Scanning and Web Application security analysis categories to discover and exploit vulnerabilities. As a blue team member students will use skills developed on the CYRIN labs in the Secure Network Setup, Network Monitoring and Recon, and Secure Web Application Setup categories to detect and block the attack.	In this exercise, as a red team member, students will use their knowledge of network recon and vulnerability scanning tools to find and exploit vulnerabilities in order to capture your "flags". As a blue team member, students will use their knowledge of network monitoring tools and secure web application setup techniques to detect the attack and block it	CYRIN labs in the Secure Network Setup, Secure System Setup, Network Monitoring and Recon, Vulnerability Scanning, Secure Web Application Setup and Web Application Security Analysis categories.	

LEVEL 3 ATTACKS

COURSE TITLE	COURSE DESCRIPTION	LEARNING OBJECTIVE	PREREQUISITES	AVAILABILITY
ICS OT Man in the Middle Attack	This attack scenario presents a man-in-the-middle attack on the OT network. Students will need to know if a device on their Operational Technology (OT) network was compromised on its way from the factory to them. Or if a contractor inadvertently installed some malware that didn't activate until months later. This scenario presents just such an attack on the OT network—one of the existing devices on the network is intercepting and modifying SCADA traffic. It could be producing false measurements, or be sending commands to an unsuspecting device on behalf of the SCADA Server! The attack starts approximately 5 minutes after the exercise begins. The students' job is to determine the nature of the attack, find its source, and neutralize it.	Students must determine the nature of the attack, find its source on the OT network, and neutralize it.	Familiarity with the UNIX command line and advanced networking concepts, as well as common OT/SCADA network protocols such as Modbus.	Currently Available
ICS IT/OT Phishing Attack	In this attack, it only takes one user clicking on a phishing e-mail to launch a devastating attack. Successful phishing attempts give an attacker access to your IT network resources, and possibly your OT network as well.This scenario presents just such an attack—one of the users on the IT side of the network has inadvertently opened a malicious e-mail attachment. What are the consequences to the IT and OT networks, and how can this be contained and neutralized?	Students must determine what the phishing attack is doing, see how far it has spread, and neutralize it.	Familiarity with the UNIX command line and advanced networking concepts, as well as common OT/SCADA network protocols such as Modbus.	Currently Available
ICS OT Application-Level DoS Attack	A Denial of Service (DoS) attack can cripple your business operations and your physical infrastructure. How will you find and stop such an attack? How will your personnel perform when the system is in a degraded state?This scenario presents just such an attack on the OT network—a DoS attack at the application layer, aimed at disrupting normal operations. This DoS attack takes place when a malicious entity generates a large number of connections to the server to block legitimate applications from connecting to the victim server.	Students must determine the nature of the attack, find its source on the OT network, and neutralize it.	Familiarity with the UNIX command line and advanced networking concepts, as well as common OT/SCADA network protocols such as Modbus.	Currently Available
ICS OT Network-Level DoS Attack	A Denial of Service (DoS) attack can cripple your business operations or your physical infrastructure. How will you find and stop such an attack? How will your personnel perform when the system is in a degraded state? This scenario presents just such an attack on the OT network—a DoS attack at the network layer, flooding your systems with bogus data and slowing operations to a crawl.	Students must determine the nature of the attack, find its source on the OT network, and neutralize it.	Familiarity with the UNIX command line and advanced networking concepts, as well as common OT/SCADA network protocols such as Modbus.	Currently Available

				COMING IN 2020
Remote Control Server in an Industrial Control Network	This attack will start with the process of reconnaissance and then move to attack surface and vector recognition. Access will be gained on one of the OT systems. Privilege escalation will be performed. Command and Control will be established between a simulated external site.	Students will setup and establish a command and control scenario using an OT existing asset.	Basic networking concepts (TCP/IP). Familiarity with the UNIX command line.	
Blended Advanced Persistent Threat (APT)	This attack will simulate the infection methods of one of the main ICS/SCADA malware. The attack will simulate the covert network command and control that the malware samples Stuxnet, Shamoon and Flame have exhibited. The last part of the exercise will be an attack that simulates the Ukraine attack with the attacker gaining control of the machine and shutting down the power grid.	Students will infect a network with one of the current ICS/SCADA malware variants to include a simulated crash of a power grid.	Basic networking concepts (TCP/IP). Familiarity with the UNIX command line.	
Malware Analysis in Industrial Control Networks	This attack includes the process of identifying the infection methods such as • Dropper • Wiper • Remoter. Also ways to determine Command and Control methods. Also includes: Analysis of conversations • Detecting obfuscation • Indicators of Compromise (IOC) identification • Applying metrics and data analysis to assign attribution • Recognizing the different APT threat groups • Detecting the malware campaign • Extracting the required data for forensics processing.	Students will observe a variety of attacks and the results of the attacks. After these observations, the student will conduct a process to collect the forensics data.	Basic networking concepts (TCP/IP). Familiarity with the UNIX command line.	