LAB LIBRARY

TRAINING FOR THE CYBER PROFESSIONALS OF TOMORROW

CYBRScore's immersive "hands-on" labs cover cyber-centric topic areas including incident response, malware analysis, computer, media and mobile device exploitation, penetration testing and vulnerability assessment, reverse engineering, information assurance and cyber forensics.

Our labs are available in a hosted on-demand environment so students learn by doing anywhere: in a classroom, workplace or at home.

PerformanScore® Enabled Library

Scored Mini-Assessments are available for select labs.

Beginner

- Auditing Service Accounts and Setting Up Automated Log Collection (Expected Duration 1 hour)
- CIRP Creation After Cyber Attacks (Expected Duration 1 hour) *Mini-Assessment Available*
- Creation of Standard Operating Procedures for Recovery (Expected Duration 1 hour, 30 minutes)
- Firewall Setup and Configuration (Expected Duration 1 hour)
- Pentesting & Network Exploitation - LINUX Target Analysis Labs (Expected Duration 3 hours)
- Pentesting & Network Exploitation - Windows Target Analysis Labs (Expected Duration 3 hours)

Intermediate

- Analyze Packed Executable to Identify Attack Vector and Payload (Expected Duration 45 minutes)
- Applying Filters to TCPDump and Wireshark (Expected Duration 1 hour)
- Conduct Root Cause Analysis for System Crashes (Expected Duration 45 minutes) *Mini-Assessment Available*
- Control Assessment and Evaluation (Expected Duration 1 hour)
- Creating Recommendations Based on Vulnerability Assessments (Expected Duration 1 hour) *Mini-Assessment Available*
- Cybersecurity Testing with Core Impact (Expected Duration 1 hour) *Mini-Assessment Available*
- Detecting Changes to System Configurations (Expected Duration 45 minutes)
- Dynamic Malware Analysis (Expected Duration 1 hour) *Mini-Assessment Available*
- Entering Information into a CMDB (Expected Duration 30 minutes)
- Fixing a Company BCP, DRP and CIRP (Expected Duration 1 hour, 30 minutes) *Mini-Assessment Available*
- Identify Rootkit and DLL Injection Activity (Expected Duration 40 minutes)
- Identifying Malicious Network Connections (Expected Duration 1 hour)
- Image Forensics (Expected Duration 1 hour, 30 minutes) *Mini-Assessment Available*

CYBRScore

PerformanScore® Enabled Library

Intermediate (continued)

- Leveraging Internal Intelligence Resources
  (Expected Duration 45 minutes) *Mini-Assessment Available*
- Log Correlation
  (Expected Duration 30 minutes) *Mini-Assessment Available*
- Monitoring Network Traffic
  (Expected Duration 1 hour)
- Patching with WSUS
  (Expected Duration 30 minutes)
- Rogue Device Identification and Blocking
  (Expected Duration 1 hour)
- Setting Up Zones in a Firewall
  (Expected Duration 1 hour)
- System Administrator (Auditing and Log Collection)
  (Expected Duration 45 minutes) *Mini-Assessment Available*
-
- Use pfTop to Analyze Network Traffic
  (Expected Duration 40 minutes) *Mini-Assessment Available*
- Using Snort and Wireshark to Analyze Traffic
  (Expected Duration 1 hour)
- Vulnerability Proof of Concept and Remediation
  (Expected Duration 1 hour) *Mini-Assessment Available*

Advanced

- Pentesting & Network Exploitation - LAN Exploitation Labs
  (Expected Duration 3 hours)
- Pentesting & Network Exploitation - WAN/DMZ Exploitation & Pivoting Labs
  (Expected Duration 3 hours)
- Penetration Tester Challenge
  (Expected Duration 3 hours) *Mini-Assessment Available*

Additional Available Labs

Beginner

- Additional Scanning Options
  (Expected Duration 45 minutes)
- Auditing Service Accounts and Creation of Service Accounts To Run Specific Services
  (Expected Duration 1 hour)
- BCP DRP and Test Planning
  (Expected Duration 4 hours)
- CIRP Creation and Disaster
  (Expected Duration 42 minutes)
- Creating a List of Installed Programs, Services and User Accounts from a WIN2K12 Server
  (Expected Duration 1 hour)
- Creation of BCP and DRP
  (Expected Duration 46 minutes)
- Data Backup to Prep for Recovery
  (Expected Duration 1 hour)
- Disable User Account on Windows 7
  (Expected Duration 45 minutes)
- Identifying Key Assets
  (Expected Duration 1 hour)
- Implement Single System Changes in Firewall
  (Expected Duration 45 minutes)
- Incident Detection and Identification
  (Expected Duration 2 hours, 30 minutes)
- Installing Patches and Testing Software
  (Expected Duration 1 hour, 30 minutes)
- Interoffice Communications Correction
  (Expected Duration 30 minutes)
- Linux Users and Groups
  (Expected Duration 1 hour)
- Manually Creating a Baseline with MD5DEEP
  (Expected Duration 1 hour)
- Microsoft Baseline Security Analyzer
  (Expected Duration 1 hour)
- Network Miner
  (Expected Duration 1 hour)
- Patches and Updates
  (Expected Duration 1 hour)
- Personal Security Products
  (Expected Duration 45 minutes)
- Report Writing for Presentation to Management
  (Expected Duration 1 hour)
- Sensitive Information Identification
  (Expected Duration 1 hour)
- Wireshark
  (Expected Duration 1 hour)

Intermediate

- Active Directory Security Checkup
  (Expected Duration 1hour, 30 minutes) *Mini-Assessment Available*
- Analysis and Recommendation Report
  (Expected Duration 2 hours)
- Analyze and Classify Malware
  (Expected Duration 1 hour)
- Analyze and Update a Company BCP/BIA/DRP/CIRP
  (Expected Duration 1 hour, 30 minutes)
- Analyze Malicious Activity in Memory Using Volatility
  (Expected Duration 38 minutes)
- Analyze SQL Injection IOC
  (Expected Duration 45 minutes)
- Analyze SQL Injection Attack
  (Expected Duration 42 minutes)
- Analyze Various Data Sources to Confirm Suspected BlackHole Infection
  (Expected Duration 1 hour)
- Assessing Vulnerabilities Post Addressal
  (Expected Duration 1 hour)
- Automated in-Depth Packet Decoding
  (Expected Duration 1 hour)
- Automated Vulnerability Assessments
  (Expected Duration 1 hour)
- Baseline Systems in Accordance with Policy Documentation
  (Expected Duration 1 hour)
- BitLocker Setup
  (Expected Duration 30 minutes)
- Block Incoming Traffic on Known Port
  (Expected Duration 1 hour)

CYBRScore

Additional Available Labs

- Centralized Monitoring (Expected Duration 1 hour)
- Check for Indicators of Other Attack Activity (Debug PE File) (Expected Duration 1 hour, 30 minutes)
- Clonezilla_Network (Expected Duration 46 minutes)
- Collecting Logs and Verifying SYSLOG Aggregation (Expected Duration 1 hour, 30 minutes)
- Comparing Controls (Expected Duration 1 hour)
- Comprehensive Threat Response (Expected Duration 2 hours)
- Compromise Assessment with Crowd Response (Expected Duration 48 minutes)
- Conduct Baseline Comparison for Indicators of Compromise (Expected Duration 1 hour)
- Conduct Log Analysis and Cross Examination for False Positives (Expected Duration 1 hour)
- Conduct Supplemental Monitoring (Expected Duration 30 minutes)
- Core Impact Vulnerability Scan (Expected Duration 2 hours)
- Core Impact Web Application Penetration Testing (Expected Duration 1 hour)
- Create Custom Snort Rules (Expected Duration 1 hour)
- Creating a Baseline Using the Windows Forensic Toolchest (WFT) (Expected Duration 30 minutes)
- Creating a Secondary Baseline and Conducting Comparison (Expected Duration 1 hour)
- Creating SEIM Reports with Splunk (Expected Duration 1 hour)
- Data Recovery with Autopsy (Expected Duration 30 minutes)
- Detect the Introduction and Execution of Malicious Activity (Expected Duration 1 hour)
- Detect Unauthorized Changes Comparing Approved Configurations (Expected Duration 1 hour, 30 minutes)
- DNS as a Remote Shell (Expected Duration 1 hour)
- DOS PCAP Analysis (Expected Duration 1 hour, 13 minutes)
- Event Log Collection (Expected Duration 1 hour)
- Gap Analysis of Firewall Rules (Expected Duration 1 hour, 30 minutes)
- Holistic Network Identification and Protection (Expected Duration 2 hours)
- Host Compromise Identification Scanning (Expected Duration 1 hour, 30 minutes)
- Host Data Integrity Baselining (Expected Duration 1 hour)
- Host Identification Scanning via Windows (Expected Duration 25 minutes)
- Host Identification Scanning with Linux (Expected Duration 1 hour)
- Identify Access to a LINUX Firewall Through SYSLOG Service (Expected Duration 20 minutes)
- Identify Additional Activity - Rootkit and DLL Injection (Expected Duration 1 hour) *Mini-Assessment Available*
- Identify and Remove Trojan Using Various Tools (Expected Duration 45 minutes)
- Identify Suspicious Information in VM Snapshots (Expected Duration 1 hour)
- Identify Whether High-Risk Systems Were Affected (Expected Duration 1 hour)
- Identifying Anomalous ARP (Expected Duration 1 hour)
- Identifying Intrusion and Mitigating Attacks with RHEL Server (Expected Duration 45 minutes)
- Identifying Malicious Callbacks (Expected Duration 1 hour)
- Identifying System Vulnerabilities with OpenVAS (Expected Duration 1 hour)
- IDS Setup and Configuration (Expected Duration 1 hour, 30 minutes)
- Implementing Least-Privilege on Windows (Expected Duration 45 minutes)
- Install EMET and Edit Host Files (Expected Duration 1 hour)
- Live Imaging with FTK Imager Lite (Expected Duration 45 minutes)
- Log Analysis (Expected Duration 45 minutes)
- Log Correlation and Analysis (Expected Duration 49 minutes)
- Log Event Reports (Expected Duration 1 hour)
- Manual Vulnerability Assessments (Expected Duration 1 hour)
- Manually Analyze Malicious PDF Documents (Expected Duration 1 hour)
- Manually Analyze Malicious PDF Documents 2 (Expected Duration 1 hour, 30 minutes)
- Memory Extraction and Analysis (Expected Duration 1 hour, 54 minutes)
- Monitoring and Verifying Management Systems (Expected Duration 1 hour)
- Monitoring for False Positives (Expected Duration 1 hour)
- Monitoring Network Traffic for Potential IOA/IOC (Expected Duration 1 hour)
- Network Discovery (Expected Duration 1 hour, 30 minutes)
- Network Segmentation (FW/DMZ/WAN/LAN) (Expected Duration 1 hour)
- Network Topology Generation (Expected Duration 1 hour)
- Data Backup and Recovery (Expected Duration 1 hour)
- Open and Close Ports on Windows 7 (Expected Duration 1 hour)

CYBRScore

Additional Available Labs

- Open Source Collection
  (Expected Duration 2 hours)
- Open Source Password Cracking
  (Expected Duration 1 hour, 51 minutes)
- Packet Analysis and Attack Scope
  (Expected Duration 1 hour)
- Parse Files Out of Network Traffic
  (Expected Duration 1 hour)
- Participate in Attack Analysis Using Trusted Tool Set
  (Expected Duration 38 minutes)
- Patch Installation and Validation Testing
  (Expected Duration 1 hour, 30 minutes)
- Performing Incident Response in a Windows Environment
  (Expected Duration 45 minutes)
- Performing an Initial Attack Analysis
  (Expected Duration 1 hour)
- Post Incident Service Restoration
  (Expected Duration 1 hour)
- Preliminary Scanning
  (Expected Duration 1 hour)
- Protect Against Beaconing
  (Expected Duration 1 hour)
- Recover from Browser-based Heap Spray Attack
  (Expected Duration 1 hour, 17 minutes)
- Recover from Illegal Bitcoin Mining Incident
  (Expected Duration 45 minutes)
- Recover from Incident
  (Expected Duration 48 minutes)
- Recover from SQL Injection Attack
  (Expected Duration 1 hour, 6 minutes)
- Recover from Web-Based Flashpack Incident
  (Expected Duration 1 hour, 19 minutes)
- Recovering Data and Data Integrity Checks
  (Expected Duration 1 hour)
- Recovery From Inadequate Patching
  (Expected Duration 45 minutes)
- Incident Response Remove Trojan
  (Expected Duration 1 hour)
- Report Comparison and Evaluation
  (Expected Duration 1 hour)
- Respond to and Validate Alerts from Antivirus Software
  (Expected Duration 26 minutes)
- Scanning and Mapping Networks
  (Expected Duration 45 minutes)
- Scanning From Windows
  (Expected Duration 45 minutes)
- Searching for Indicators of Compromise
  (Expected Duration 1 hour)
- Securing Linux for System Administrators
  (Expected Duration 45 minutes)
- Setting Up SYSLOG Forwarding From a Windows System
  (Expected Duration 49 minutes)
- Specialized Linux Port Scans
  (Expected Duration 45 minutes)
- System Hardening
  (Expected Duration 1 hour)
- TCPDump
  (Expected Duration 1 hour)
- Techniques for Manual Malware Recovery
  (Expected Duration 1 hour)
- Threat Designation
  (Expected Duration 1 hour)
- Tweaking Firewall Rules for Detection
  (Expected Duration 1 hour)
- Using Identity Finder to Identify a System Containing Sensitive Information
  (Expected Duration 1 hour, 9 minutes)
- Using Identity Finder to Manually Search a Remote System for Sensitive Data
  (Expected Duration 1 hour)
- Using Identity Finder to Manually Search a System for Sensitive Data
  (Expected Duration 1 hour)
- Using PowerShell to Detect
  (Expected Duration 1 hour)
- Validate Alerts from Antivirus Software
  (Expected Duration 30 minutes)
- Validate Indications of Compromise: Analysis of PE File
  (Expected Duration 30 minutes)
- Verify Attributes of Identified SilentBanker Intrusion
  (Expected Duration 1 hour)
- Verify Attributes of Intrusion Through Additional Analysis
  (Expected Duration 40 minutes)
- Verifying Hotfixes
  (Expected Duration 1 hour)
- Vulnerability Analysis/Protection
  (Expected Duration 1 hour, 30 minutes)
- Vulnerability Identification and Remediation
  (Expected Duration 1 hour)
- Vulnerability Scan Analysis
  (Expected Duration 2 hours)
- Vulnerability Scanner Set-up and Configuration
  (Expected Duration 1 hour)
- Vulnerability Scanner Set-up and Configuration, Pt. 2
  (Expected Duration 1 hour)
- Whitelist Comparison
  (Expected Duration 1 hour)
- Whitelist IP Address from IDS Alerts
  (Expected Duration 1 hour)
- Whitelisting & Suspicious File Verification
  (Expected Duration 2 hours)
- Windows Deployment Services
  (Expected Duration 48 minutes)
- Windows Event Log Manipulation via Windows Event Viewer
  (Expected Duration 1 hour)

Advanced

- Advanced Techniques for Malware Recovery
  (Expected Duration 1 hour, 5 minutes)
- Analyze Browser-based Heap Spray Attack
  (Expected Duration 43 minutes)
- Analyze Structured Exception Handler Buffer Overflow Exploit
  (Expected Duration 32 minutes)
- Detect Embedded Shellcode in a Microsoft Office Document
  (Expected Duration 1 hour)

CYBRScore

Tools Utilized Throughout CYBRScore® Labs

- Active Domain
- All MSFT
- Apache
- Armitage
- Bro
- Core Impact
- CU Spider
- ELSA
- Foxit PDF reader
- MS - EMET (Enhanced Mitigation Experience Toolkit)
- Hping-win3
- md5deep
- Metasploit
- Metasploitable
- mmc (Microsoft Management Console)
- MS Baseline Analyzer
- MS Security Essentials
- MS Baseline Security Analyzer
- MySQL
- Network Miner
- Nmap
- OpenVAS Manager (v4.0.5)
- OpenVAS Client (V3.0.3)
- OpenVAS Administrator (v1.3.2)
- pfsense firewall
- PHP
- Python 2.7
- Scanline
- Security Essentials
- Server Backup
- Snorby
- Snort
- Splunk
- Suricata
- tcpdump
- Windows firewall
- Windows offline updater
- Win 7 SP1 installer
- Wireshark
- Zenmap

CYBRScore