TECHNICAL SYSTEMS INTEGRATORS

CYBRScore® Skills Lab Library

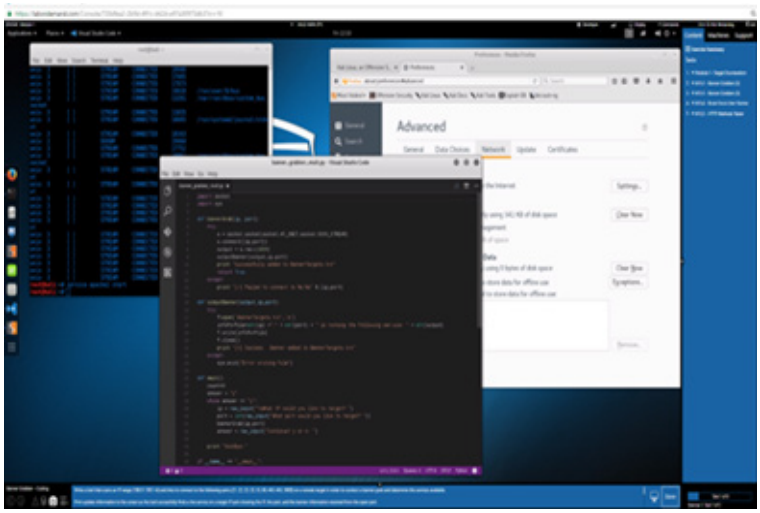
TRAINING FOR THE CYBER PROFESSIONALS OF TOMORROW

CYBRScore's immersive hands-on labs allow professionals to develop and enhance their skills in an independent fashion. Our library includes over 300 labs in a variety of topic areas including system hardening, vulnerability analysis, incident response, digital media forensics, malware analysis, and penetration testing as well as general IT skills. Labs are available in a hosted environment that can be accessed ***on-demand anywhere, anytime***.

CYBRScore labs are delivered in 3 formats. **Step-by-step labs** provide sufficient instructions such that they can be used as standalone learning environments. They walk the student thru the lab for structured but independent learning. **Scored labs** provide scoring results back to the instructor providing information on lab completion and amount of time spend in the lab. **Capstone labs** remove the scaffolding and test student's knowledge, skills and abilities (KSAs). Capstone labs evaluate the student in a scored scenario-based environment providing real time results.

Key benefits

- On Demand based on your schedule - Available 24x7.
- Browser Based – HTML5 – No special software, VPN, or plug-ins required.
- Turn-key, we host everything, no hardware/software or licenses to manage.
- Easily Scales to support growing workforce or student base (tens, hundreds, thousands).
- Evaluates candidate performance in real-time - Scored results returned immediately.
- Real-world scenarios – using actual operating systems and complex networks.
- Individual Learning Plans reduce training time and costs.



CYBRScore®

Lab Library (Example)

Beginner

- » 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)
- 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)

Intermediate

- Analyze SQL Injection Attack (Expected Duration 42 minutes)
- Analyze Various Data Sources to Confirm Suspected BlackHole Infection (Expected Duration 1 hour)
- Baseline Systems in Accordance with Policy Documentation (Expected Duration 1 hour)
- Core Impact Web Application Penetration Testing (Expected Duration 1 hour)
- Create Custom Snort Rules (Expected Duration 1 hour)
- Log Analysis (Expected Duration 45 minutes)
- Log Correlation and Analysis (Expected Duration 49 minutes)
- Recover from Illegal Bitcoin Mining Incident (Expected Duration 45 minutes)
- Recover from Incident (Expected Duration 48 minutes)

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)
- 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

Available Lab Bundles

Custom Lab Bundles Built On-Request

- Network Essentials
- Security Essentials
- Ethical Hacker Essentials
- Security Professional Essentials
- Pentesting & Network Exploitation
- Pentest Module 1 Windows Target Analysis
- Pentest Module 2 LINUX Target Analysis
- Pentest Module 3 LAN Exploitation
- Pentest Module 4 DMZ Exploitation
- Digital Media Forensics Basic
  Digital Media Forensics Advanced
- Digital Media Forensics Network
- Protocol Analysis
- Intrusion Detection
- Incident Handing Methodology
- Network Defense
- Network Attack
- Information Gathering
- Attack (Red Team)
- Defend (Blue Team)

Tools Utilized Throughout CYBRScore® Labs

- Apache
- Armitage
- bro
- Core Impact
- CU Spider
- DarkComet RAT
- ELSA
- Foxit PDF reader
- Hping3
- Kali
- md5deep
- Metasploit
- Microsoft Baseline Security Analyzer
- mmc (Microsoft Management Console)
- MS Baseline Analyzer
- MS Security Essentials
- MySQL
- Network Miner Nmap
- OpenVAS
- pfsense firewall
- PHP
- Python 2.7
- Scanline
- Security Essentials
- Server Backup
- Snorby
- Snort
- Splunk
- Suricata
- tcpdump
- Win 7 SP1 installer
- Windows Firewall
- Windows offline updater
- Wireshark
- Zenmap

About CYBRScore®

Comtech Mission Critical Technologies (Comtech MCT) provides cybersecurity solutions and services tailored to training and workforce development. The CYBRScore® product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech MCT CYBRScore® offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

CYBRScore®
Technical Systems Integrators, Inc.
www.tsieda.com
(407) 339-4874, x102

TECHNICAL SYSTEMS INTEGRATORS