Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
	Labs Overview
	Lab Introduction and Access
	Using the Clipboard
	Using IML Kali Client
Cyber Awareness	Cyber Terminology
	Ethics
	Cyber Introduction
	Cyber Kill Chain
	Wifi Hotspots
	Shoulder Surfing
	Social Media and Privacy
	Passwords
	Patching / Updating
	Malware
	Phishing Emails
Cyber Investigator	Investigator Operations Security (OPSEC)
	TOR and TOR Hidden Services
	Domain Intel
	Default Credentials
	Google Searching
	Robots.txt
	Reverse Image Search
	Exif
	Open Source Interests
	OSINT Social Media
	OSINT: Deleted Tweet
Compliance	GDPR Aware
	GDPR Aware - Practice
Information Assurance	Introduction to Information Assurance
	Risk Management
	Qualitative and Quantitative Risk Management
	Accreditation
Linux Command Line	Moving Around
	Changing Things
	Package Management
	Going Places
	Getting Hashed
	Stream Redirection
	Clever Counting
	Sudo
	Text Editors
	Combining Commands
	Searching
	Regular Expressions

Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
	Manipulating Text
Networking	Dynamic Host Configuration
	Internet Protocol v4
	Internet Protocol v6
	Automatic Addressing with IPV6
	Domain Names
	TCP
	UDP
	Ports
Windows Operating Systems	File Permissions
	Scheduled Tasks
	Windows Registry
	Policies
	Environment Variables
	Alternate Data Streams
Security Engineering	Intrusion Detection Systems
	Accounting and Audit
Encoding and Encryption	Binary
	Symmetric Key Encryption
	Caesar Cipher
	Hashing – SHA1
	Base64 Encoding
	Hashing – MD5
	Hexadecimal
	ASCII
	Steganography
Kali	Kali at Home
	Kali Web Desktop
	The Basic: Msfvenom
	The Basics: Msfconsole Multihandler
	SearchSploit
	Nikto/ dirb
	Msfconsole: Hydra
Burp Suite	Intro To Burp Suite
	Into to Web Proxy Servers
Common Tool Sets	Introduction to John The Ripper
	Meltdown Proof of Concept
	Volatility Level 1
	Volatility Level 2
	Volatility Level 3
	Volatility Level 4
	Volatility Level 5
	Mimikatz Primer
	SIFT Introduction
Wireshark	Introduction to Wireshark

Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
	Wireshark Setup
	Wireshark
	BPF Syntax
	TLS Decrypt
	Stream Extraction
	Ducky PCAP Analysis
Top 10 OWASP PHP	PHP A1 – Injection Flaws
	PHP A2 – Broken Authentication and Session Management
	PHP A3 – Cross Site Scripting
	PHP A4 – Insecure Direct Object References
	PHP A5 – Security Misconfiguration
	PHP A6- Sensitive Data Exposure
	PHP A7 – Missing Function Level Access Control
	PHP A8 – Cross Site Request Forgery
	PHP A9 – Using Vulnerable Components
	PHP A10 – Unvalidated Redirects and Forwards
Top 10 OWASP Java	Java OWASP A1 – Injection
	Java OWASP A2 – Broken Authentication and Session Management
	Java OWASP A3 – Cross Site Scripting (XSS)
	Java OWASP A4 – Broken Access Control
	Java OWASP A5 – Security Misconfiguration
	Java OWASP A6 – Sensitive Data Exposure
	Java OWASP A7 – Insufficient Attack Protection
	Java OWASP A8 – Cross Site Request Forgery (CSRF)
	Java OWASP A9 – Using Components with Known Vulnerabilities
	Java OWASP A10 – Underprotected APIS
Top 10 OWASP C# / ASP.NET	ASP.Net OWASP A1 – Injection
	ASP.Net OWASP A2 – Broken Authentication and Session Management
	ASP.Net OWASP A3 – Cross Site Scripting
	ASP.Net OWASP A4 – Broken Access Control
	ASP.Net OWASP A5 – Security Misconfiguration
	ASP.Net OWASP A6 – Sensitive Data Exposure
	ASP.Net OWASP A7 – Insufficient Attack Protection
	ASP.Net OWASP A8 – Cross Site Request Forgery
	ASP.Net OWASP A9 – Components with Known Vulnerabilities
	ASP.Net OWASP A10 – Under protected API's
Ethical Web Hacking	Unsafe Mantis
	Unrestricted File Upload
	Web Applications: Source Code Review
	Web Applications: HTTP Parameters and I.P.
	Web Applications: Directory Traversal
	Web Server: Brute Force Authentication
	Cross Site Request Forgery

Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
	Dynamic Typed Language – PHP
	Web Applications: SQL Injection
	Web Applications: Blind SQL Injection
	SQL Injection / File Download
	Command Execution
	Heartbleed
	Open Source: Juice Shop
	Apache Web Server
	Git Creds
	MongoDB Mini CTF – Ethical Web Hacking
	Apache Basic Authentication
Ethical Infrastructure Hacking	Shadow Brokers Victim
	Ethical Infrastructure Hacking: Network Scanning
	Banner Grabbing
	Netcat
	Vulnerable Application Services – FTP
	Password Hashes 1
	Password Hashes 2
	DNS Enumeration
	Brute Force Authentication – MySQL, Postgres, HTTP, FTP, SSH
	SMTP User Enumeration
	SNMP
	ShellShock
	Port Knocking
	Linux Logon Script
	Linux Privilege Escalation and Routing Modifications
	Linux Host: Privilege Escalation Config Error 1
	Linux Host: Privilege Escalation Config Error 2
	WEP Cracking
	WPA Cracking
	Windows Service Privilege Escalation
	Pass The Hash
Cyber SOC Analyst	Punycode / Homograph
	Packet Capture Basics
	Packet Capture – Key Extraction
	Server Identification
	Honeypot Interaction
	Log Finder
	MongoDB
	Windows Internal Misuse Investigation
	Suspected Compromise: BSD9
	Forensic Malware Analysis
	Event Analysis
	Event Analysis 2
	SMTP Log Analysis

Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
	RAT Attack
	Web Log Analysis
Cyber Coding and Security	C Code Audit
	C Sharp Reverse Engineering and Web Authentication Bypass
	Basic Stack Manipulation
	Stack Overflow
	Python Coding – Network Challenge Level 1
	Python Coding – Network Challenge Level 2
	Python Coding – Network Challenge Level 3
	Python Coding – Network Challenge Level 4
	Java Encryption
	Pseudo Random Number Generator (PRNG) – Java
IoT/Embedded	What is IoT and Cyber?
	Real world examples of IoT/Embedded security issues
	IoT/Embedded Network Protocols and Security
	IoT/Embedded hardware reverse engineering
	IoT Best Practice
	Firmware Credentials
	Certificate Underpinning
Threat Hunting	Windows Odd One Out
	Mining Behaviour
	Yara Rules
Malware Analysis	Windows Ransomware
	Wannacry
	Petrwrap
	Kovter Trojan
	Bad Rabbit
	DarkComet
	Annabelle
	Malware Documents
Digital Forensics & Incident Response	Introduction to Forensics
	Introduction to Incident Response
	The Incident Response Process
	Legal Side
	Windows Forensics
	Ubuntu Image Analysis
	Windows Artefacts
	Suspicious Email
	Prior Attack
	BitLocker Encrypted Drive
Reverse Engineering	Introduction to ELF Reverse Engineering
	ELF Execution Structure
	Introduction to Assembly

Cyber Security Labs

Lab Packages

Cyber Modules	Lab Name
Threat Hunting	Introduction to Threat Hunting
	Windows Odd One Out
AWS Security	S3 Security Permissions
	AWS Security Groups
Cyber Warrior: CTF	Immune Hacking Group
	Mallory Coffee Shop
	Pasting Place
	Walter
	Binary Analysis – 5 Part Mini Series
	Mini CTF's – A collection of challenges
	Immersive Bank Mini-Series
	Immersive Construction
	Incident Response CTF
	Pen Test CTF
Originals	ASLR Bypass – Written by Pedro Ribeiro
	Linux File System Race Conditions
	Reverse Engineering