CyberSecurity Pass

Updated as of March 12, 2024

Novice

Security

Security+ Domain 4: Security Operations II	8:33:43
Security+ Domain 4: Security Operations I	9:36:34
Security+ Domain 3: Security Architecture	8:34:48
Security+ Domain 2: Threats, Vulnerabilities & Mitigations	10:59:06
Security+ Domain 1: General Security Concepts	8:39:15
Secure Architecture Design	5:30:57
Security+ Domain 5: Security Program Management & Oversight	None

Penetration Testing

Assessment Methodologies: Footprinting & Scanning	11:16:04

Blue Team

Defensive Security Concepts	10:13:31
Cloud Security Principles	5:31:57
Introduction to Ransomware	1:51:22
Incident Handling in the Cloud with AWS	4:00:59
Incident Handling in the Cloud Fundamentals	4:03:20

PCAP to XML and SQLITE	0:06:03
Memcache Reconnaissance for Red-Blue Teams	1:34:02

Red Team

Introduction to Web Application Security Testing	11:23:05
Introduction to Vulnerability Management	7:05:57

Cyber Security Engineering

Security Engineering for Business Operations	1:38:57
Security Engineering and System Hardening Bootcamp	7:52:03

Enterprise Governance & Risk

Introduction to Identity & Access Management (IAM)	5:31:50
Introduction to Security & Risk Management	6:48:59

Online Bootcamp

The Metasploit Framework Bootcamp	9:47:46

INE Fundamentals Pass

Assessment Methodologies: Information Gathering	5:14:38
Assessment Methodologies: Enumeration	12:14:43
Assessment Methodologies: Auditing Fundamentals	2:14:57
Host & Network Penetration Testing: System/Host Based Attacks	20:29:47
Host & Network Penetration Testing: Exploitation	20:49:25
Host & Network Penetration Testing: Post-Exploitation	26:33:16
Host & Network Penetration Testing: The Metasploit Framework (MSF)	39:29:18

Web Application Penetration Testing: Introduction to the Web and HTTP Protocol	9:05:39

Network Defense

Introduction to Security Sensors & Logging Management	6:30:26

Cyber Security Hardening

Introduction to Cyber Security Hardening	7:34:16
Fundamentals of Penetration Testing Concepts	7:48:19

Countermeasure Coordination & Impact Analysis

Introduction to Security Engineering & Change Management	3:56:16

Exploit Development

Windows Exploit Development	10:08:01
Linux Exploit Development	11:50:00

Firewall

Palo Alto Firewall Technologies	8:38:42
Palo Alto Firewall Policies	5:08:56
Palo Alto Firewall Essentials	3:41:34

Security Engineering & Change Mgmt

Perimeter & Network Security Engineering	6:33:41

Pentester Academy

Airodump-NG Scan Visualizer	None
Traffic Analysis: TSHARK Unleashed	0:27:51
Scripting Wi-Fi Pentesting Tools in Python	2:10:53

Pentesting Challenges	0:03:32
Pentesting with Metasploit	6:16:36

Professional

None

Asset Security for CISSP	5:47:41
Security & Risk Management for CISSP	6:57:46
Actionable Information from Aggregated Log Data	6:39:35
Webapp Security Bootcamp	11:09:25

Security Engineering & Change Mgmt

Email Security Management & Strategy	7:05:57
Active Directory Security Configuration & Management	6:58:02
Authentication, Authorization, & Identity Engineering	6:25:03
PKI Design	6:32:49

Red Team

Web Application Security Testing: Web Service Security Testing	5:29:46
Web Application Security Testing: CMS Security Testing	9:01:28
Web Application Security Testing: Testing for Common Attacks	12:00:50
Web Application Penetration Testing: File & Resource Attacks	10:40:15
Web Application Penetration Testing: SQL Injection Attacks	16:47:23
Web Application Penetration Testing: XSS Attacks	8:52:35

Web Application Penetration Testing: Web Fingerprinting and Enumeration	10:38:56

Security Assessments

WAPT: Web Proxies and Web Information Gathering	12:32:50

Pentester Academy

DevSecOps Bootcamp	11:10:15
WiFi Pentesting Bootcamp	11:04:18
Container Security Bootcamp	9:20:50
AWS Cloud Security Bootcamp	16:49:49
Linux Privilege Escalation Bootcamp	10:06:29
WAP Challenges	4:44:16
Pentesting iOS Applications	4:01:44
Javascript for Pentesters	1:17:57
Wi-Fi Security and Pentesting	19:54:54
iOS Penetration Testing: The Basics	0:26:54
Hacker Project: SMS Controlled Pentest Bot	0:18:24
Python for Pentesters	10:06:44
OSINT: Fun with Open Source Intelligence	2:07:10
Pandas for Pentesters	3:58:48
Make Your Own Hacker Gadget	1:45:03
Web Application Pentesting	7:27:23

Exploit Development

Penetration Testing: Exploitation and Post-Exploitation Tactics	21:51:41

Blue Team

Digital Forensics: File & Disk Analysis	5:49:08
Digital Resistance: Basic Incident Response with a Wartime Focus Bootcamp	5:48:27
Incident Handling and Response Process for AWS Cloud Bootcamp	5:30:28
Digital Forensics & Incident Response in the Cloud Bootcamp	5:16:26
Digital Forensics: Introduction & Acquisition	5:13:47
Digital Forensics: Logs, Timelines & Reporting	2:10:41
Digital Forensics: System & Network Forensics	13:09:07
Digital Forensics: Introduction & Acquisition	3:53:08
Threat Hunting: Hunting the Endpoint & Endpoint Analysis	13:48:51
Threat Hunting: Hunting the Network & Network Analysis	4:20:34
Digital Forensics: File & Disk Analysis	10:19:54
Incident Handling & Response: Network Traffic & Flow Analysis	3:00:00
Introduction to Threat Hunting	3:18:52
Practical Incident Handling	1:40:00
Incident Handling & Response: SOC 3.0 Operations & Analytics	3:42:28
Malware Analysis	16:51:02
Practical Reverse Engineering	10:32:07

Reverse Engineering Foundations	1:20:00
Linux Forensics	8:04:07
DevSecOps: Insecure Docker Registry	0:11:44
USB Forensics and Pentesting	1:19:41
VoIP Traffic Analysis	5:00:13
Windows Forensics	10:03:47

Incident Handling & Response

IHRP Cloud Foundations Bootcamp	4:28:19

Online Bootcamp

Assessment Methodologies Bootcamp	4:50:48
Cloud Pentesting Bootcamp	6:03:04
Recon and Vulnerability Detection Bootcamp	8:03:17

INE Fundamentals Pass

Assessment Methodologies: Vulnerability Assessment	2:46:22
Host & Network Penetration Testing: Network-Based Attacks	4:31:34
Host & Network Penetration Testing: Social Engineering	1:31:55

Penetration Testing

eCPPTv2 Exam Preparation	1:15:08
Penetration Testing: Metasploit & Ruby	7:51:47
Penetration Testing: Wi-Fi Security	5:14:15

Penetration Testing: Web App Security	9:44:56
Penetration Testing: Linux Exploitation	8:41:08
PowerShell for Pentesters	5:59:01
Penetration Testing: Network Security	32:44:36
Penetration Testing: System Security	12:20:36
iOS & Mobile App Pentesting	4:53:53
Android & Mobile App Pentesting	6:13:32
Client-Side Attacks	None
Wireless Security	None
Command & Control (C2/C&C)	None
Active Directory Penetration Testing	None
Web Application Penetration Testing	None
Exploit Development with Metasploit & Ruby	None
Privilege Escalation	None
Lateral Movement & Pivoting	None
System Exploitation	None
PowerShell for Pentesters	None

Cyber Security Hardening

Network Security Auditing Basics	3:05:52
Securing Windows Endpoint Devices	6:49:02

Firewall

Palo Alto Firewall Advanced Technologies	7:30:17
Palo Alto Firewall Advanced Policies	7:26:38

Web Defense

Practical Web Defense	40:30:37

Security

Identity & Access Management for CISSP	None
Security Operations for CISSP	None
Communication & Network Security for CISSP	None
Security Assessment & Testing for CISSP	None
Software Development Security for CISSP	None
Security Architecture & Engineering for CISSP	None

Advanced

Red Team

Web Application Security Testing: Encoding, Filtering & Evasion Basics	8:01:06
Web Application Penetration Testing eXtreme	18:22:31

Blue Team

Windows System Programming: Security	3:49:39
Windows System Programming: Memory Management	3:32:13
Windows System Programming: Processes and Threads	3:36:35

Windows Kernel Programming: Fundamentals	3:12:41
Windows Kernel Programming: Processes and Threads Monitoring	2:44:57
Embedded/IoT Linux for Red-Blue Teams	6:57:13
Reverse Engineering Win32 Applications	14:51:02
Linux Rootkits for Red-Blue Teams	3:44:40
Reverse Engineering Linux 32-bit Applications	8:38:58
Windows System Programming: Fundamentals	3:50:01
GNU Debugger Megaprimer	3:50:47
Reverse Engineering for ARM Platforms	1:49:53
ARM Assembly	5:27:32
WinDbg Fundamentals: User Mode	2:32:39
WinDbg Fundamentals: Kernel Mode	0:12:30
Wi-Fi Monitoring for Red-Blue Teams	1:20:53

Cyber Security Hardening

Active Directory Protection & Tiering	6:31:11
Azure Pentesting	6:42:31

Penetration Testing

Penetration Testing: Preparing the Attack	2:03:30
Penetration Testing: Red Teaming Active Directory	4:30:28
Penetration Testing: Red Teaming Critical Domain Infrastructure	3:23:42

Penetration Testing: Evasion	0:20:00

Pentester Academy

Windows Process Injection for Red-Blue Teams	3:00:27
x86_64 Assembly Language and Shellcoding on Linux	5:13:59
Data Science and Machine Learning for Infosec	13:41:38
Exploiting Simple Buffer Overflows on Win32	3:50:00
Windows API Exploitation Recipes: Processes, Tokens and Memory RW	3:18:06

Linux Programming

x86 Assembly Language and Shellcoding on Linux	6:02:45