CompTIA Cybersecurity Analyst CySA+ (CS0-003)

This intermediate CompTIA Cybersecurity Analyst CySA+ (CS0-003) training prepares security professionals for the CySA+ exam, which is needed to earn the to Cybersecurity Analyst certification. Learn security skills like how to proactively monitor devices and networks and detect malicious activity using up-to-date methods and tools.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Introduction to CySA+ — 159 min.

Getting our tools ready	6
Putting an OS inside of VirtualBox	7
Installing the Kali operating system in VirtualBox	9
Booting into our Virtual Operating System (Kali)	9
Metasploit	4
Wrapping up with a Practical Challenge	5

Security in the System and Network Architecture

Security within the Architecture	1
Identity and Access Management	12
Encryption and Sensitive Data Protection	11
Data at Rest or Data in Motion?	1
Data Loss Prevention (DLP)	8
Challenge	9

Indicators of Potentially Malicious Activity

Indicators of Potentially Malicious Activity	2
Where do we get our alerts from?	10
Looking more at active and passive.	5
Understanding Event Capturing and Forwarding	6
Verifying our Network	3
Focusing on the weird things	8
Security Information and Event Management (SIEM)	3
The human aspect	3

Techniques to Determine Malicious Activity

Diving deeper into the traffic	9

WEEK 2

154 min.

Traffic Capturing and Wireshark

System Services and Analysis

Security Response Systems

Threat Hunting and Intelligence Concepts

WEEK 3

152 min.

Improvement in Security Operations

Vulnerability Scanning Methods

Vulnerability Tool Assessment

Understanding our Assessment Results	7
Can we duplicate it?	14
Let's scan with OpenVAS	10
Discrepancies???	5

WEEK 4

154 min.

Challenge	8

Prioritize Vulnerabilities

Knowing the Priority	9
What's the Risk?	4
Looking at the CVSS 3.0 Vector	6
Sometimes a suggestion (Context Awareness)	6
Common Vulnerabilities	8
Challenge	11

Controls to Mitigate Vulnerabilities

Controlling the Vulnerabilities	4
Easy path first	11
Network Segmentation and ACLs	12
Adding Multiple Layers of Security	3
Is it the User's Fault??	2
Audit and Logging	3
Incident Response	2
Challenge	5

Vulnerability Response and Handling

Understanding Incident Handling and Response	6
Preparation	11
Detection and Analysis	5
Containment, Eradication, and Recovery	7
Post-Incident Activity	3
Challenge	9
Addendum	1

Attack Methodology Frameworks

Understanding the Attack	4
MITRE ATT&CK Framework	14

WEEK 5

159 min.

The Diamond Model	9
The Cyber Kill Chain	13
Challenge	9

Incident Response Activities

What Triggers Incident Response?	6
Indicators of a Compromise	10
Compromise Investigation	7
Preserving Evidence	7
Challenge	13

Incident Management Life Cycle

What is Digital Forensics?	3
What our Toolkit Consists of	3
FTK	15
Imaging Devices	4

Network Forensics	9
Challenge	10

Vulnerability Management Reporting

Vulnerability Management Reporting	6
Mitigation	7
Action Planning	8
Stakeholders	7
Reporting	13

WEEK 6

12 min.

Challenge	11
Ultimate Challenge	1

Last updated 12.3.2024