kaspersky
expert training

CYBER THREAT HUNTING

Course
program

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
0	Course overview	• About your trainers • Course roadmap • Course structure	—		Course introduction	—
					Introduction to virtual lab	—
1	Introduction to Threat Hunting	• Threat hunting as an analytical process • How to use MITRE ATT&CK as a behavioral reasoning framework • Types of hunting • How to translate operational threat intelligence into huntable hypotheses	• TTP hunting • WMI consumer hunting • Linux service hunting • Domain anomaly hunting • Endpoint anomaly hunting • APT report hunting	Threat Hunting	Introduction to Threat Hunting	—
					Threat Hunting as an Analytical Discipline	—
					MITRE ATT&CK as a Hunting Framework	—
					Threat Hunting Telemetry	—
					Security Monitoring	Knowledge check: security monitoring
					Hypothesis-Driven Threat Hunting	—
					Threat intelligence	—
				Labs	Threat Hunting Walkthrough	
					Windows WMI Consumer Hunting	Quiz
					Linux Service Hunting	Quiz
					Anomaly Hunt: Behavioral Deviation on a Workstation	Quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Labs	Domain Name Hunting	Quiz
					APT-report Hunting: Intelligence-Driven Hunt Based on External Threat Report	Quiz
					Mid-module quiz	Checkpoint quiz
2	Windows Environment Threat Hunting	• Windows OS main cybersecurity features • Processes, places and sensitive information storage • Kerberos attacks and exploitation • Windows Active Directory audit management • Preventing account manipulation, privilege escalation and lateral movement • Mapping offensive activities onto logs • Using Velociraptor to validate hypotheses	• Searching for the actions of adversaries from the logs • Matching attacking techniques with the MITRE ATT&CK matrix • Using Windows audit for investigations • Correlating suspicious activity • Reconstructing multi-stage attack chains from behavioral evidence	Windows credentials and authentication	SAM and NTDS DIT. Part 1	Knowledge check: SAM and NTDS DIT. Part 1
					Lab: Password credentials in SAM and NTDS	Quiz
					SAM and NTDS DIT. Part 2	Knowledge check: SAM and NTDS DIT. Part 2
					Lab: Password credentials in memory	Quiz
					SAM and NTDS DIT. Part 3	Knowledge check: SAM and NTDS DIT. Part 3
				Labs	Lab: Security support providers	Quiz
					Lab: User rights	Quiz
					Lab: Windows services exploitation	Quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Windows privileges	Privileges and access control Lab: Windows privileges	Knowledge check: privileges and access control
					UAC Lab: UAC	Knowledge check: UAC
					Pass the token Lab: Pass the token and Impersonation	Knowledge check: pass the token
				Kerberos	Kerberos principles	Knowledge check: Kerberos
					Kerberoasting Lab: Kerberoasting	Knowledge check: Kerberoasting Quiz
					AS-REP roasting Lab: AS-REP roasting	Knowledge check: AS-REP roasting
					Silver ticket Lab: Silver ticket	Knowledge check: Silver ticket Quiz
					Golden ticket Lab: Golden ticket	Knowledge check: Golden ticket Checkpoint quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Windows security auditing	Windows security auditing Lab: Windows Security Auditing	Knowledge check: Windows security auditing Quiz
				Threat Hunting in Windows	Threat Hunting in Windows	—
				Labs	TTP-Hunting in Windows №1 Suspicious Multi-Stage Activity in the Domain	Quiz
					TTP Hunt in Windows №2: Suspected Targeted Intrusion in Financial Sector Environment	Quiz
					Velociraptor: Suspicious Post-Compromise Activity on a Workstation	Quiz
					Mid-module quiz	Checkpoint quiz
3	Linux security, attack vectors and hunting	• Linux general info: distros, package management, important features, etc. • Linux security components • Linux monitoring • Linux capabilities and auditing system • Common Linux persistence and execution patterns	• System tool privilege abuse hunting and investigation (openssl) • Auditd telemetry for hunting and investigation • Sudo misconfiguration abuse hunting and investigation • Hunting privilege escalation through SUID/SGID abuse • Tracing SSH-based lateral movement	Linux general information	Linux Security, Attack Vectors and Hunting	—
				Linux security	Linux security	—
				Mandatory access control	Mandatory access control	—
				Labs	Lab: Openssl	Quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
					Lab: Sudo privilege escalation	Quiz
				Threat Hunting in Linux	Threat Hunting in Linux	—
				Labs	TTP Hunt in Linux №1: Suspected Web Server Compromise in Logistics Sector Environment	Quiz
					TTP Hunt in Linux №2: Suspected CI/CD Infrastructure Breach and Supply Chain Tampering	Quiz
					Mid-module quiz	Checkpoint quiz
4	Network threat hunting	• Basics of network technologies • Common approaches to the network security • Network security monitoring • Specialized network devices • Key network data sources for threat hunting • How to hunt for command-and-control channels, lateral movement, and data exfiltration in network telemetry	• Investigation spoofing and replying attacks • Investigation server-side attacks	Introduction to networks	Introduction to networks	—
				Typical network attack	Typical network attacks	—
				Network security monitoring tools	Network security monitoring tools	—
				Labs	Spoofing and replying. Investigation with Wireshark and Zeek	Quiz
					Client-side attack	Quiz
					Server-side attack	Quiz
				Threat Hunting in Network	Threat Hunting in Network	—
					Course summary	—
					Mid-module quiz	Checkpoint quiz

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky