

kaspersky
expert training

Suricata for incident response and threat hunting

Course
program

Nº	Track	What you will learn/practice	Lesson	Practice	Evaluation
0	Course overview	<ul style="list-style-type: none"> About your trainer Course roadmap Course structure 	Introduction	—	—
1	Suricata basics	<ul style="list-style-type: none"> Basic information about network protocols What is NIDS? The principles of their work and their main functions Most popular NIDS and the differences between them Useful tools for network traffic analysis 	How to run Suricata in virtual lab	Network and NIDS basics	Checkpoint quiz
			How Suricata works?	Exercise 1 Solution to Exercise 1	—
2	Rules writing basics	<ul style="list-style-type: none"> Structure and syntax of Suricata rules Basic keywords Selecting good options for a rule 	Writing basic rules	Exercise 2: rule writing basics Solution to Exercise 2	Checkpoint quiz
3	Writing rules for HTTP protocols	<ul style="list-style-type: none"> Specific keywords for HTTP protocols How to write a rule step-by-step Writing rules for an HTTP protocol for a given traffic dump 	HTTP content keywords	—	Checkpoint quiz
			Writing rules for CopperStealer spy	Lab 1 Solution to Lab 1	—
			Writing rules for HQWar Android dropper	Lab 2 Solution to Lab 2	—

Nº	Track	What you will learn/practice	Lesson	Practice	Evaluation
4	Writing rules for DNS, TSP and SSL/TLS protocols	<ul style="list-style-type: none"> • Basic information about DNS, TCP and SSL/TLS protocols • Keywords and tips for writing rules for these protocols • Writing rules for DNS, TCP and SSL/TLS protocols for a given traffic dump 	Writing rules for DNS	Lab 3: writing rules for DNS Solution to Lab 3	—
			DNS tunneling	Lab 4: DNS tunneling Solution to Lab 4	—
			Writing rules for TCP protocol	Lab 5: writing rules for TCP Solution to Lab 5	—
			Writing rules for SSL/TLS protocol	Lab 6: writing rules for SSL/TLS Solution to Lab 6	Checkpoint quiz
5	Advanced Suricata features	<ul style="list-style-type: none"> • Advanced rule options that aren't always necessary but can help a lot in some cases • Selecting best options for a rule • Writing rules for a given traffic dump 	Advanced Suricata features. Part 1	Lab 7: advanced Suricata features Solution to Lab 7	Quiz
			Advanced Suricata features. Part 2	—	—
6	Detecting typical attacks	<ul style="list-style-type: none"> • About popular network attacks and how to detect them • Writing rules to detect typical attacks for a given traffic dump 	Ransomware, Phishing, Coinmining	Lab 8 Solution to Lab 8	Quiz
			Reconnaissance, Exploits, APT	Lab 9 Solution to Lab 9	Checkpoint quiz

Nº	Track	What you will learn/practice	Lesson	Practice	Evaluation
7	Problem solving	<ul style="list-style-type: none"> • About typical problems when writing Suricata rules and how to solve them • How to check rule performance • How to fix false positives • How to write “good” rules • Solving typical problems • Fixing false positives 	Performance issues. False alarms	Lab 10 Solution to Lab 10	—
			Circumventing precise rules and solving other problems	—	Checkpoint quiz
8	Course project	<ul style="list-style-type: none"> • Self-writing rules for a given traffic dump from scratch 	—	Lab 11 Solution to Lab 11	—
9	Course summary	<ul style="list-style-type: none"> • Brief summary of the course • Trainer's closing remarks 	Summary	—	—

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky