kaspersky
expert training

Advanced malware reverse engineering with Ghidra

Course
program

№	Track	What you will learn/practice	Lesson	Practice/Evaluation
0	Course overview	• About your trainer • Course roadmap • Course structure	Introduction	—
			Virtual lab introduction	—
1	Introduction to Ghidra	• The process of setting up Ghidra • Building its latest version from source code	Ghidra overview	—
			Building Ghidra on Windows, macOS, Linux	—
2	Analysis workflow	• How to perform a typical malware analysis workflow with Ghidra	Introduction to the sample: Metasploit	—
			Creating a new Ghidra project	—
			Settings overview, configuring familiar controls	—
			Basic analysis workflow	—
			Using Data Type Manager to import type libraries	Analysis workflow: challenge Checkpoint quiz Analysis workflow: solution
			Analysis workflow: track summary	
3	Working with types and pointers	• How to work with data types and structures in Ghidra	Linked lists and adjusting shifted pointers	Linked lists and adjusting shifted pointers: challenge Quiz Linked lists and adjusting shifted pointers: challenge solution

№	Track	What you will learn/practice	Lesson	Practice/Evaluation
			The case for the MZ and PE headers: variables in the same register	—
			Creating variables in the listing with scripting	Creating variables in the listing with scripting: challenge Checkpoint quiz Creating variables in the listing with scripting: challenge solution
			Working with types and pointers: track summary	—
4	Scripting API hashing	• How to perform API hash resolution in general • How to iterate over assembly instructions with Ghidra and extract operand values from them • How to set comments and equates using Ghidra's scripting capabilities	Scripting API hashing: introduction	—
			API hashing algorithm analysis	—
			Implementing API hashing recovery in Python: setting comments	—
			Implementing API hashing recovery in Python: setting equates	—
			Implementing API hashing recovery in Java	Scripting API hashing: challenge Quiz Scripting API hashing: challenge solution Checkpoint quiz
			Scripting API hashing: track summary	—

№	Track	What you will learn/practice	Lesson	Practice/Evaluation
5	Library identification	• How to identify library code with Ghidra • How to use Ghidra's Headless Mode	Introduction to the sample: Mettle	—
			Creating a function ID database from an executable	—
			Creating a function ID database from multiple object files with Headless mode	Library identification: challenge Quiz Library identification: challenge solution Checkpoint quiz
			Library identification: track summary	—
6	Structures and function pointers	• How to auto-create structures with Ghidra • How to expand structures in the decompilation window • How to deal with structure members that are function pointers	Introduction to the sample: Calypso	—
			Starting the analysis	—
			Applying function pointers in structures	Structures and function pointers: challenge Quiz Structures and function pointers: challenge solution Checkpoint quiz
			Structures and function pointers: track summary	—
7	Decompiler scripting	• Internals of Ghidra's decompiler • Ghidra's decompiler API • Scripting stack strings using the decompiler API	Decompiler scripting: introduction	—
			Ghidra's decompiler internals	—

№	Track	What you will learn/practice	Lesson	Practice/Evaluation
			Building stack strings	Decompiler scripting: challenge Quiz Decompiler scripting: challenge solution Checkpoint quiz
			Decompiler scripting: track summary	—
8	Final project: coding an analyzer	• How to extend Ghidra's capabilities using the Eclipse IDE™	Coding an analyzer: introduction	—
			Coding an analyzer: configuring the environment	—
			Coding the analyzer: setting comments	—
			Coding the analyzer: setting equates	Coding an analyzer: challenge Quiz Challenge solution Checkpoint quiz
			Coding the analyzer: track summary	—
9	Course summary	• Trainer's closing remarks	Course summary	—

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky