Reverse Engineering

CR113

05
Days

Reverse Engineering

Outline

This course covers reverse engineering, and provides students with the knowledge & practical training needed to excel at one of the most desired skills in hacking.

The course teaches students about malware activity, and how to bypass limitations, such as anti-debugging and VM detection techniques. Lessons in the course provide in-depth coverage of the many methods used in reverse engineering.

Topics include Assembly language, CPU & RAM architecture, malware disassembly & debugging, program patching, anti-debugging, and VM detection.

Target Audience

- SoC analysts and incident responders.
- Junior level penetration testers.
- System security personnel who are interested in learning about reverse engineering.

Prerequisites

Before attending this course, students must have the following technical knowledge:

- Working knowledge of Windows OS, Linux OS, and information security.
- Programing background in C, Python, or Java.

Objectives

Upon completing this course, students will be able to:

- Disassemble, debug, and analyze malware.
- Manipulate malware functions.
- Bypass basic anti-debugging mechanisms.
- Bypass underlying VM detection mechanisms.

Content

Day 1 Module 01 Hello Assembly

- What is Assembly
- CPU architecture
- Registers types & structure
- Commands in RAM & RAM's structure
- Stack & Heap
- Comparisons - cmp, zf instructions
- Basic C
- Introduction to IDA

Day 2 Module 02 Malware Disassembly

- IDA overview
- Jumping between display
- Code-flow analysis
- Code segments
- Variables identifications
- Arithmetic identification
- Conditions identification

Day 3 Module 03 Malware Debugging

- Debugging process
- Software & Breakpoint
- ollyDBG overview
- Following the stack
- Stepping

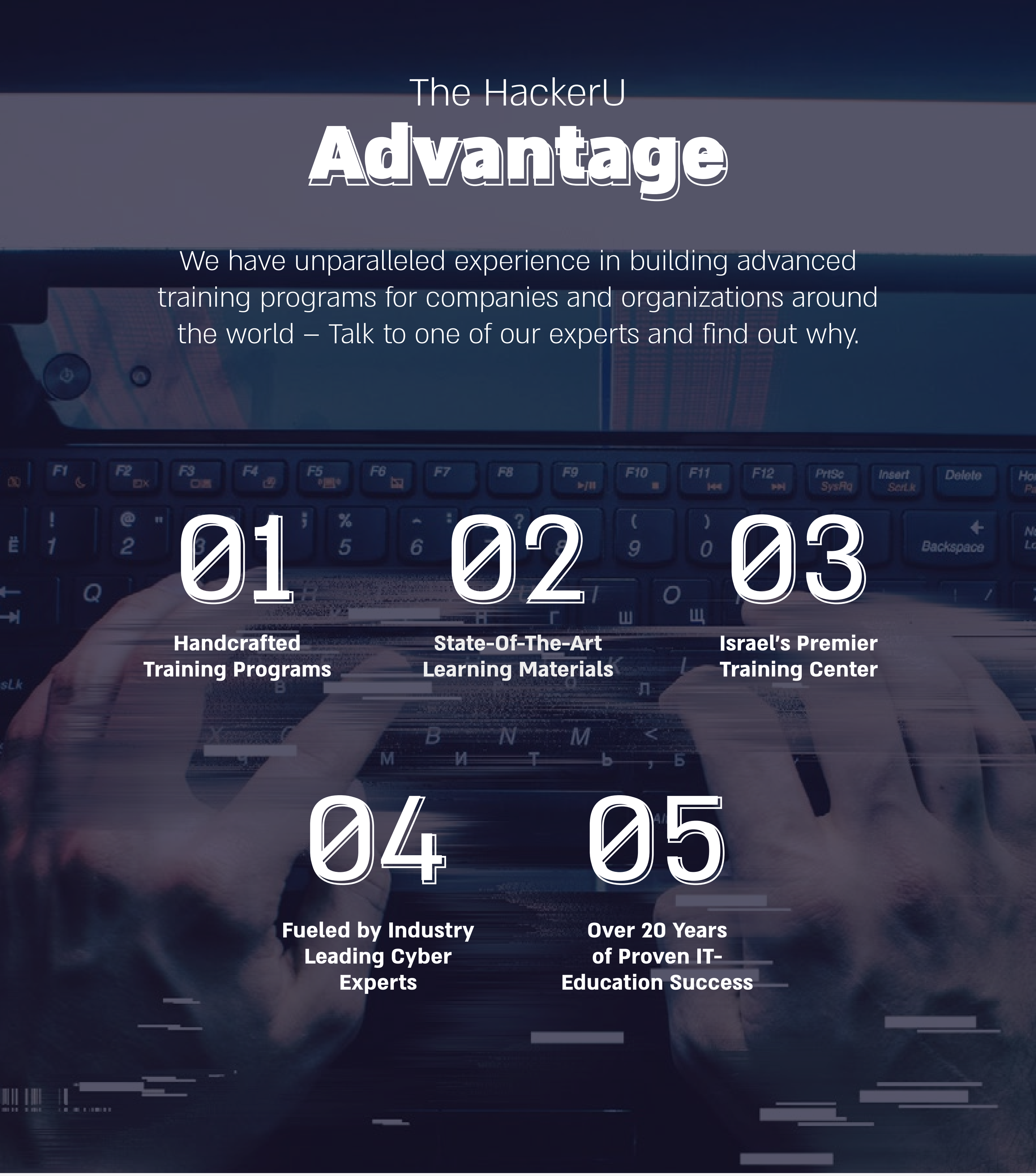
Day 4 Module 04 Patching & Anti-debugging

- Combined analysis
- Runtime manipulation
- Changing code-flow
- Patching

Day 5 Module 05 Patching & Anti-debugging

- Anti-debugging
- PEB
- VM detection
- Anti-debugging & VM detection Bypass

> "**Bypass** underlying VM detection mechanisms"



The HackerU Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world – Talk to one of our experts and find out why.

01

Handcrafted Training Programs

02

State-Of-The-Art Learning Materials

03

Israel's Premier Training Center

04

Fueled by Industry Leading Cyber Experts

05

Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

hackerupro.com