HACKERU

Windows Internals

32
Academic Hours

Windows Internals

Outline

The Windows OS exposes many advanced services to system programmers through the Windows API, and to device driver writers through the Kernel API. The .NET framework wraps these services and runs on top of the Windows API and the Kernel.

Good knowledge of what's going on under the hood of the OS, which services are available and how to best utilize them helps in building better and more efficient software for Windows. This course discusses the internal workings of Windows and its exposed services, so they can be leveraged better by developers, while gaining crucial insight for troubleshooting and debugging as well.

Target Audience

Power users that want to understand how the Windows system works, its various mechanisms, and have ways to analyze various scenarios when these occur.

Prerequisites

- Basic knowledge of OS concepts and architecture.
- C reading knowledge is beneficial

Objectives

Understand the underlying mechanism and advanced services of the windows OS and use that knowledge to understand system mechanics, process and thread operations and analyze issues.

Content

Module 01
System Architecture

- Brief Windows NT History
- Basic Concepts
- Windows Versions
- Tools: Windows, SysInternals, Debugging Tools for Windows
- Processes and Threads
- Virtual Memory
- User mode vs. Kernel mode
- Objects and Handles
- Architecture Overview
- Key Components
- User/kernel transitions
- Introduction to WinDbg
- Lab: Task manager, Process Explorer, WinDbg

Module 02
Processes & Jobs

- Process Internals & Data Structures
- Creating and terminating processes
- The loader
- Process attributes
- Protected processes and PPL
- UWP Processes
- Minimal and Pico processes
- Jobs
- Nested jobs
- Labs: viewing process and job information

Module 03
Threads

- Thread basics
- Creating threads
- Processor Groups
- Thread Priorities
- Thread Scheduling
- Threads and Performance
- Performance Counters
- Thread Stacks
- Thread States
- Thread Synchronization
- Lab: viewing thread information; Performance Monitor; Windows Performance Recorder/Analyzer

Module 04
Memory Management

- Overview
- Small, large and huge pages
- VMM Services
- Page states
- Address Space Layou
- Address Translation Mechanisms
- Heaps
- Page Faults
- Page Files
- Workings Sets
- Memory Mapped Files
- Page Frame Database
- Other memory management features
- Lab: viewing memory related information

Module 05
Kernel Mechanisms

- Trap Dispatching
- Interrupts & Exceptions
- System Crash
- Basic crash dump analysis
- Object Management
- Objects and Handles
- Sharing Objects
- Synchronization
- Synchronization Primitives
- Signaled vs. Non-Signaled
- Windows Global Flags
- Kernel Event Tracing
- Wow64
- Lab: Viewing Handles, Interrupts; Analyzing a crash dump

Module 06
Management Mechanisms

- The Registry
- Services
- Starting and controlling services
- Windows Management Instrumentation
- Lab: Viewing and configuring services; Process Monitor

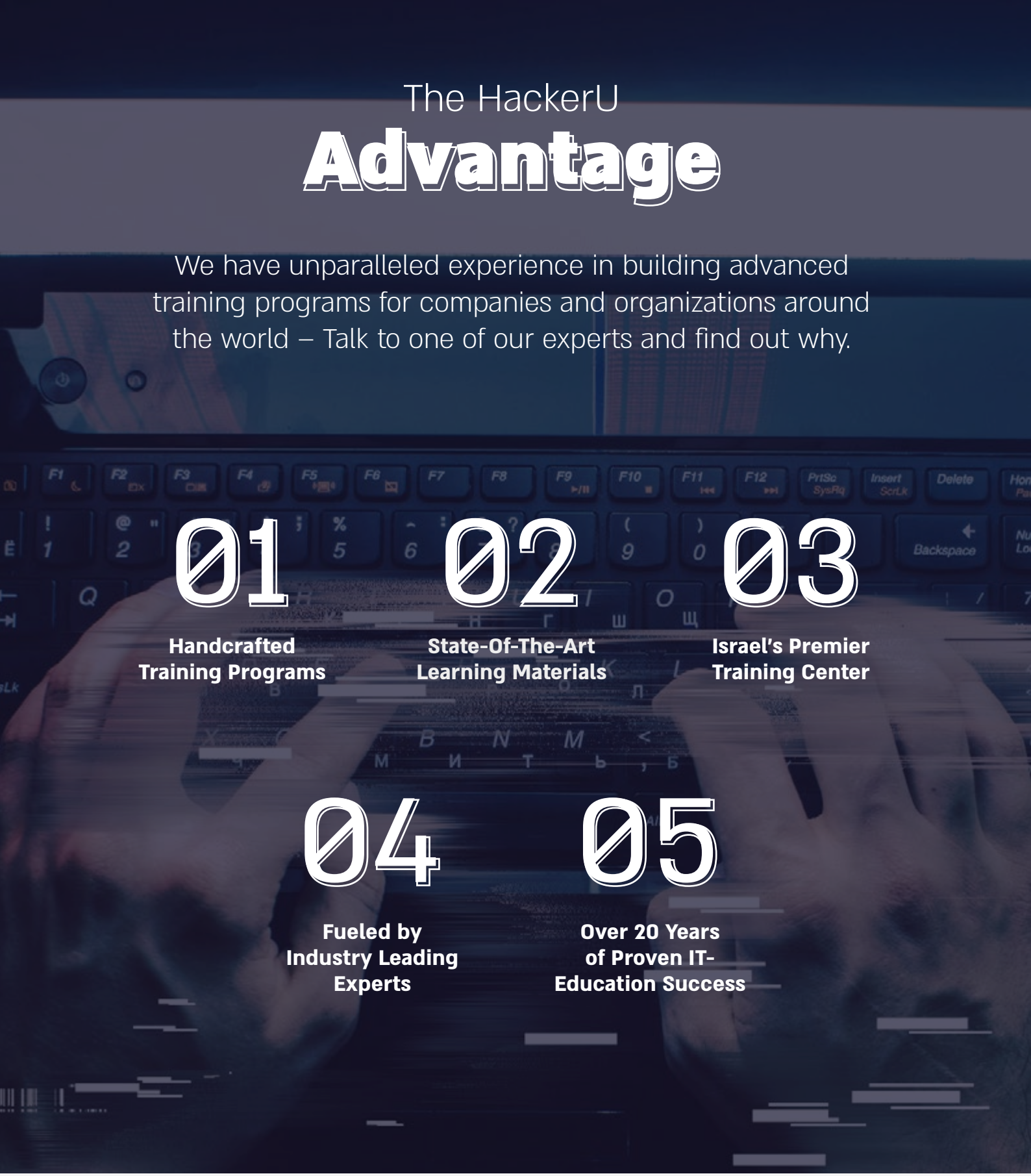
Module 07
I/O System

- I/O System overview
- I/O Function
- Device Drivers
- I/O Processing and Data Flow
- IRPs
- Plug & Play
- Power Management
- File systems and mini-filters
- Driver Verifier
- Labs: viewing driver and device information; kernel debugging

Module 08
Security (if time permits)

- Security components
- Protecting objects
- SIDs
- Token
- ACLs
- Access checking
- Privileges
- AppContainers
- Logon
- User Access Control (UAC)
- Process mitigations
- Lab: viewing security information

"Understand the **underlying mechanism and advanced services** of the windows OS"



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 Experts

05

Over 20 Years of Proven IT-Education Success

info@hackerupro.com

www.hackerupro.com