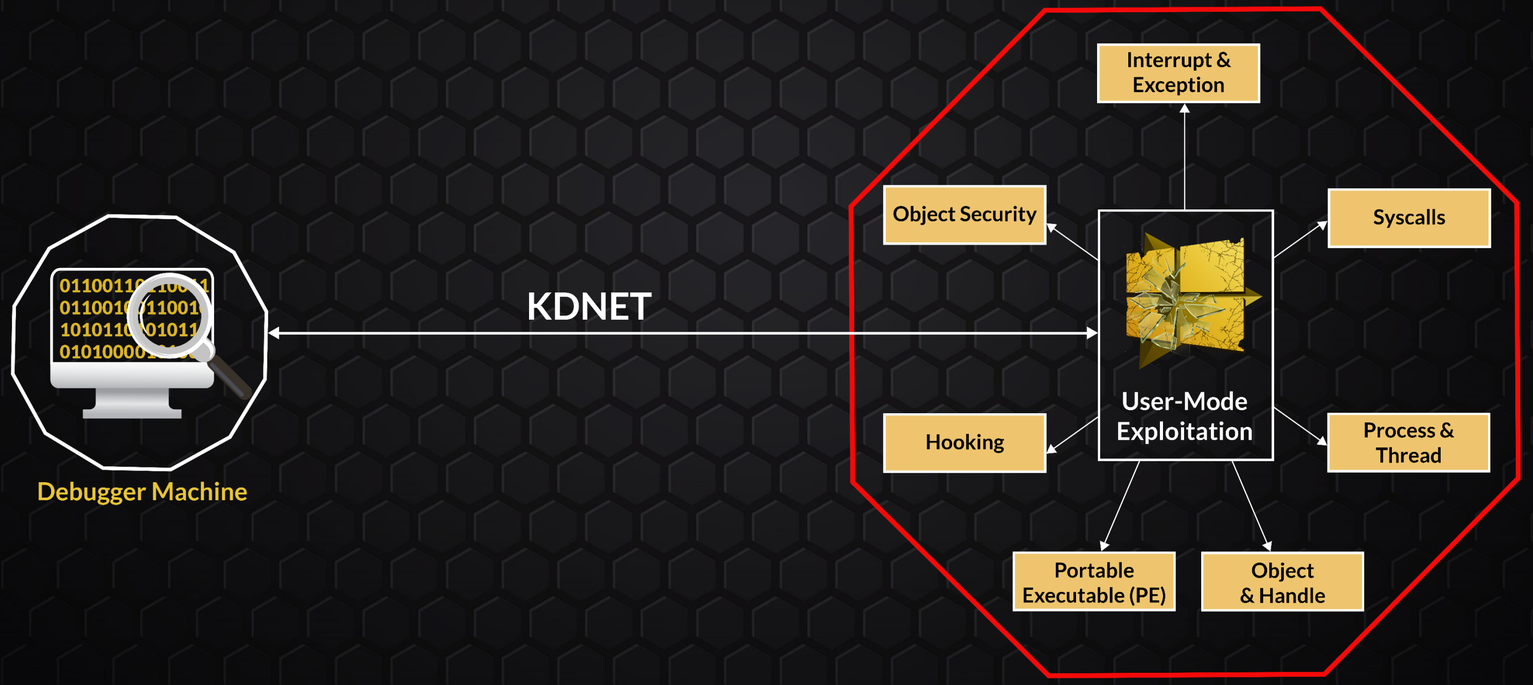
CWL

CyberWarFare Labs

Certified Windows Internals Red Team Operator [CWI-RTO]

@CyberWarFare Labs

Windows Internals Red Team Operator Architeture



CWL
CyberWarFare Labs

Windows Architecture

- Executive/Kernel/HAL/Privilege rings
  - Overview of Windows Architecture

KERNEL MECHANISMS

Kernel Mechanisms

- Interrupts & Exceptions
  - Exploring how Interrupts and Exceptions are handled
  - Labs & exercises

SYSCALLS

Syscalls

- Exploring how system calls are handledExploring
  - Labs & exercises

ASYNCHRONOUS PROCEDURE CALL (APC)

Asynchronous Procedure Call (APC)

- Exploring the APC internals
  - Labs & exercises

OBJECT & HANDLES

Object & Handles

- Analyzing relation between object and handles
  - Labs & exercises

PROCESS & THREADS

Process & Threads

- Analyzing process and threads internal strucutres EPROCESS, KPROCESS etc.
  - Analyzing process creation and thread creation
    - Labs & exercises

PE FORMAT

Pe Format

- Exploring the PE format
  - Labs & exercises

HOOKING

Hooking

- IAT Hooking
  - Labs & exercises
    - Detour Hook
      - Labs & exercises

OBJECT SECURITY

Object Security

Privilege/Token/SID/Security Descriptors

- Exploring how the object is secured by the kernel
- Labs & exercises (partial)

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live