Windows Internals

Objetivo

O objetivo deste curso é preparar profissionais avançados no desenvolvimento de software que queiram entender como componentes chaves do sistema operacional Windows funcionam internamente. O curso ajuda a escolher a tecnologia mais adequada a ser aplicada em uma solução e a entender o comportamento por trás das câmeras do sistema auxiliando na depuração de problemas complexos.

Público alvo

Este curso é destinado aos desenvolvedores de software, administradores de sistemas ou estudantes que precisam entender os conceitos fundamentais sobre arquitetura Windows, seu funcionamento interno de recursos avançados, técnicas de depuração e utilização de ferramentas de diagnóstico.

Pré-requisitos

- Conceitos básicos de Sistemas Operacionais.
- Este curso aborta tópicos avançados sobre o sistema que podem exigir o prévio conhecimento de alguns conceitos de computação para seu completo entendimento.
- Embora desenvolvedores de software tenham mais familiaridade com os conceitos apresentados, este não é um curso de programação em nenhuma linguagem de programação será utilizada durante seus exercícios.

Metodologia

Os tópicos abordados são distribuídos em 40 horas de maneira simplificada e gradativa, onde cada novo tópico utiliza os conceitos vistos em tópicos anteriores. O curso é ministrado em laboratórios onde os alunos realizarão experiências práticas que comprovarão os conceitos vistos em aula. O curso é todo apresentado em slides e acompanha material impresso.

Tópicos abordados

1) Arquitetura do Sistema
   a) Versões do Windows
   b) Conceitos Gerais
   c) Modelo do Sistema Operacional
   d) Componentes do Sistema

2) Funcionamento do Sistema
   a) Interrupções, Timers e Exceções
   b) Gerenciador de Objetos
   c) Sincronismo
   d) Threads de Sistema
   e) Flags Globais
   f) Chamada de Procedimento Assíncrono (APC)
   g) Win32 on Windows 64 (Wow64)
   h) Suporte a Debug
   i) Hypervisor
   j) Gerenciador de Transações
   k) Proteção de Patch do Kernel

3) Mecanismos de Gerenciamento
   a) O Registro
   b) Serviços
   c) Gerenciador de Processos de Fundo
   d) WMI

4) Processos, Threads e Jobs
   a) Por Dentro de um Processo
   b) Fluxo de Criação de um Processo
   c) Por Dentro de um Thread
   d) Agendamento de Threads
   e) Jobs

5) Segurança
   a) Componentes de Segurança
   b) Proteção de Objetos
   c) Direitos e Privilégios
   d) Tokens de Processo e de Thread
   e) Auditoria
   f) Logon do Sistema

g) Controle de Contas de Usuário (UAC)

6) Rede
   a) Arquitetura de Rede do Windows
   b) APIs de Rede
   c) Suporte a Redirecionamento
   d) Sistemas de Arquivo Distribuídos
   e) Resolução de Nomes
   f) Drivers de Protocolo
   g) Drivers de NDIS
   h) Camadas de Serviços de Rede

7) Sistema de I/O
   a) Componentes do Sistema
   b) Drivers de Dispositivos
   c) Processamento de I/O
   d) Kernel Mode Driver Framework (KMDF)
   e) User-Mode Driver Framework (UMDF)
   f) Gerenciador de Plug-And-Play
   g) Gerenciamento de Energia

8) Gerenciamento de Armazenamento
   a) Drivers de Disco
   b) Gerenciamento de Volumes
   c) Criptografia de Disco
   d) Serviço de Shadow Copy

9) Gerenciamento de Memória
   a) Serviços de Gerenciamento de Memória
   b) Heaps de Kernel Mode
   c) Gerenciador de Heaps
   d) Espaço de Endereçamento Virtual
   e) Tradução de Endereços (Virtual x Físico)
   f) Page Faults
   g) Pilhas
   h) Descritores de Endereço Virtual (VAD)
   i) Sections
   j) Working Sets

10) Gerenciamento de Cache
   a) Recursos do Gerenciador de Cache