USB Forensics and Pentesting

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy:
http://www.PentesterAcademy.com

USB Basics: Device Classes & Commands

Device Classes

- Answers the question “What kind of device is this?”
- Common device classes
  - Human Interface Device (HID)
  - Audio
  - Printer
  - Mass Storage

Commands: Standard

- All devices must respond to standard commands (requests)
  - Get/set address
  - Get status
  - Get/set descriptor
  - Clear/set feature
  - Get/set configuration

Commands: Class

- Commands that only make sense for certain kinds of devices
- Allows all devices of a specific type to be treated the same by OS
- Shifts driver development away from manufacturer

Commands: Vendor-specific

- Vendors may extend standard functionality for a device class
- Not commonly used

Device Class Demo