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

Human Interface Devices

What is a HID

- Keyboard
- Mouse
- Joystick
- Anything with a button
- Something that moves bytes

How does HID Work

- Boot protocol used before operating system loaded
- Report mode used once USB is up
- Report types
  - Input
  - Output (optional)
  - Features (optional)

Endpoints

- Control
- Interrupt In
- Interrupt Out (optional)

HID Descriptors

- Describe HID reports
- Boot protocol reports
  - Fixed length
  - Only for keyboard and mouse

Detecting HID Attack Devices

- Many key loggers and HID attack devices are implemented with microcontrollers
- Most support only boot protocol
- Some have well known VID/PID
- Some attempt file transfer with rarely used protocol
- Some are composite devices

HID Demo