USB Forensics and Pentesting

Dr. Phil Polstra   @ppolstra

PhD, CISSP, CEH   http://philpolstra.com

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

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

USB Basics: Connecting

USB Connections

- Device is connected
- Hub detects
- Host (PC) is informed of new device
- Hub determines device speed capability as indicated by location of pull-up resistors
- Hub resets the device
- Host determines if device is capable of high speed (using chirps)
- Hub establishes a signal path
- Host requests descriptor from device to determine max packet size
- Host assigns an address
- Host learns devices capabilities
- Host assigns and loads an appropriate device driver (INF file)
- Device driver selects a configuration

USB Connection Demo