

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 Challenge 2 - HID

The Challenge

- Identify all HID devices in the capture file
- For each device determine
 - VID/PID
 - Number of Configurations
 - Number of Interfaces
 - For each interface
 - Protocols supported
 - Endpoints
 - Determine if the device is a “real” HID