USB Forensics and Pentesting

Dr. Phil Polstra
PhD, CISSP, CEH

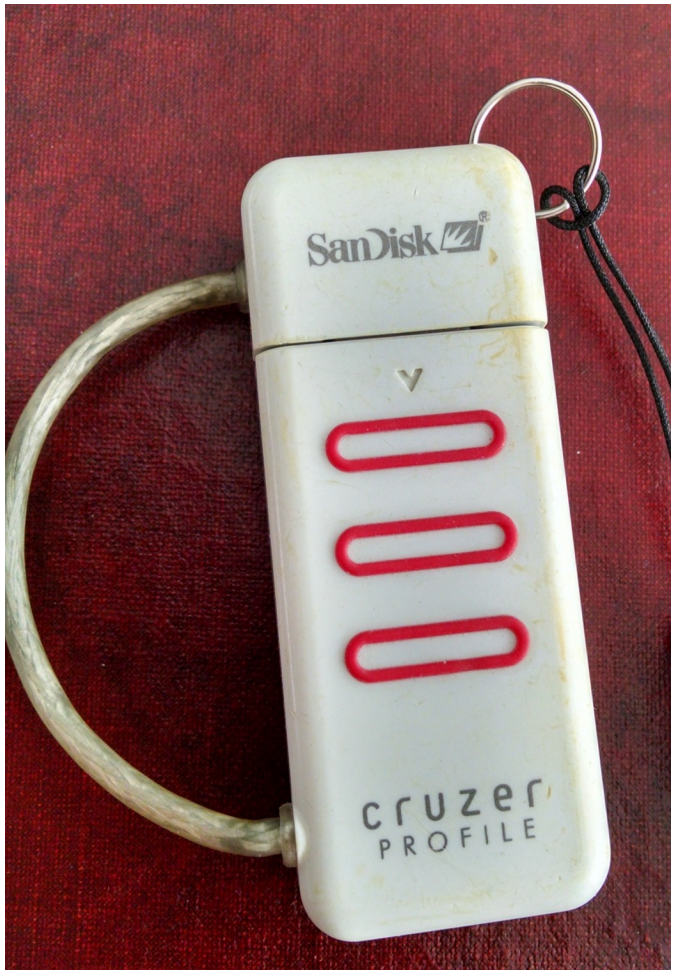
@ppolstra
http://philpolstra.com

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

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

Dealing with Windows-only Devices

Example Device



Outline of Technique

- Run Windows in a virtual machine
- Plug in device to collect VID/PID
- Create a filter in VirtualBox
- Run modprobe usbmon
- Start WireShark
- Reinsert the device w/ Windows running in VirtualBox
- Sniff and reverse engineer!

Windows-only Device Demo