

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 Answers

The Challenge

- Examine the pcapng files attached
- Determine what kind of device is being sniffed, who made it, etc.
- Some devices may be composite devices (multiple device classes in a single physical device)

Details to find

- Manufacturer & Product name
- Vendor & Product ID
- Number of configurations
- For each configuration
 - Number of interfaces & max power
 - For each interface
 - Class, subclass, protocol
 - Number of endpoints
 - For each endpoint
 - Address, type, direction

Using Wireshark to find Answers