The DIY Cybersecurity Engineer's Toolkit Part 1: Building Blocks

Presented 19 January 2019

Mark Heinrich, CISSP

Jeff Tomkiewitz, CEH

Dennis Schorn, CISSP

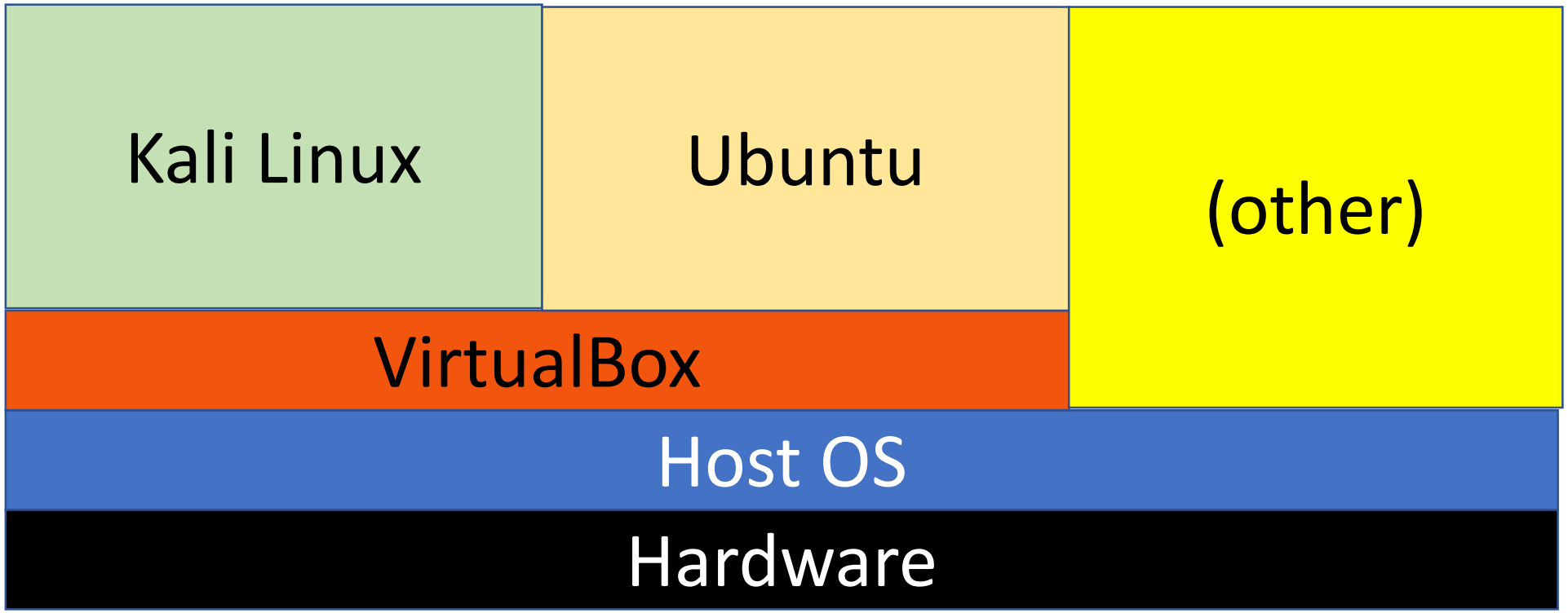
Goals

1. Load Basics
2. Open VirtualBox
3. Install, Configure Kali Linux
4. Install, Configure Ubuntu Linux
5. Test WireShark

Cautionary Notes

- Laptops are different
  - 8 GB RAM, 60 GB free on HD
- Assumptions may cause “odd” results
- Take notes
- Contribute

Overview



Load Basics

1. Load media onto laptop
2. Unzip (if needed)
3. Install VirtualBox

Kali Linux Values (iso)

1. VM name: Kali_lnx
2. Memory Size: 2048 MB
3. Create Virtual HD Now
4. HD file type : VDI
5. Storage on Phys. HD: Dynamically allocated
6. File Loc & size: VM name, 8 GB

(ova)

- Tools
- Import

Kali Linux VM Values (iso)

1. VM name: Kali_lnx
2. Memory Size: 4096 MB
3. Create Virtual HD Now
4. HD file type : VDI
5. Storage on Phys. HD: Dynamically allocated
6. File Loc & size: VM name, 8 GB

Kali Linux VM Initialization

1. Select machine, Start
2. Identify location of .iso
3. Right/Ctrl to release mouse
4. …. Hostname 0-9, alphabetic
5. Domain Name: MyLab (will use more)
6. Root password >>>KISS<<< “toor”
7. Partition disks: Guided – use entire disk
8. http proxy: (blank)

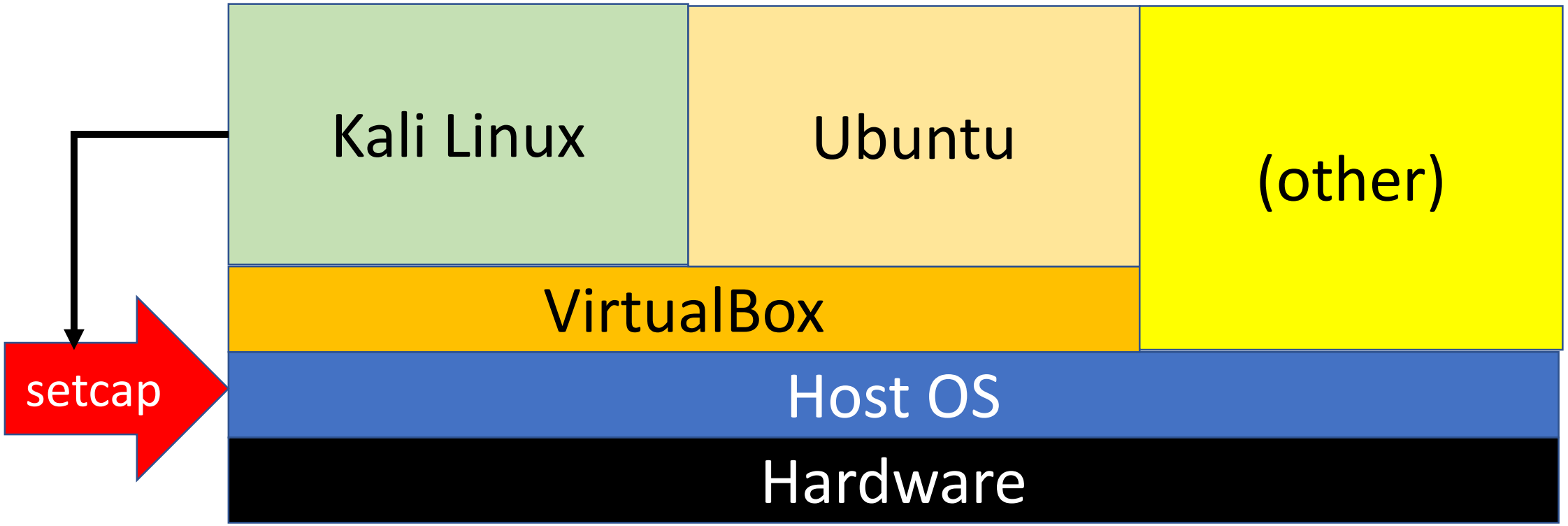
Prep Kali for Network

1. Go to Settings
2. Under Network: select Adapter 1
3. Enable it
4. On dropdown, select Promiscuous “Allow All”
5. “OK”

Prep Kali for WireShark (1/N)

1. Start system
2. Login as “root”
3. Add user wireshark
4. Add wireshark to /etc/sudoers
5. Set Wireshark ???
    1. ALL=(ALL:ALL) ALL

Setting the communication



Prep Kali for WireShark (2/N)

1. Prepare “setcap”

Prep Host OS

Open Wireshark

Send Messages & View on Wireshark