

IFS4103 Lab 1A: VM, Kali Linux and Burp Suite

Sufatrio

Overview of Tasks

- Please set up your **pen-testing environment** consisting of:
 - **VirtualBox/VMware**
 - **Kali Linux:** on top of VirtualBox/Vmware
 - **Burp Suite:**
 - Either on your Kali Linux or your host machine (Windows, Linux, Mac)
 - Either as a JAR or with an installation process
 - Either Community edition or Professional

Virtualization with VirtualBox

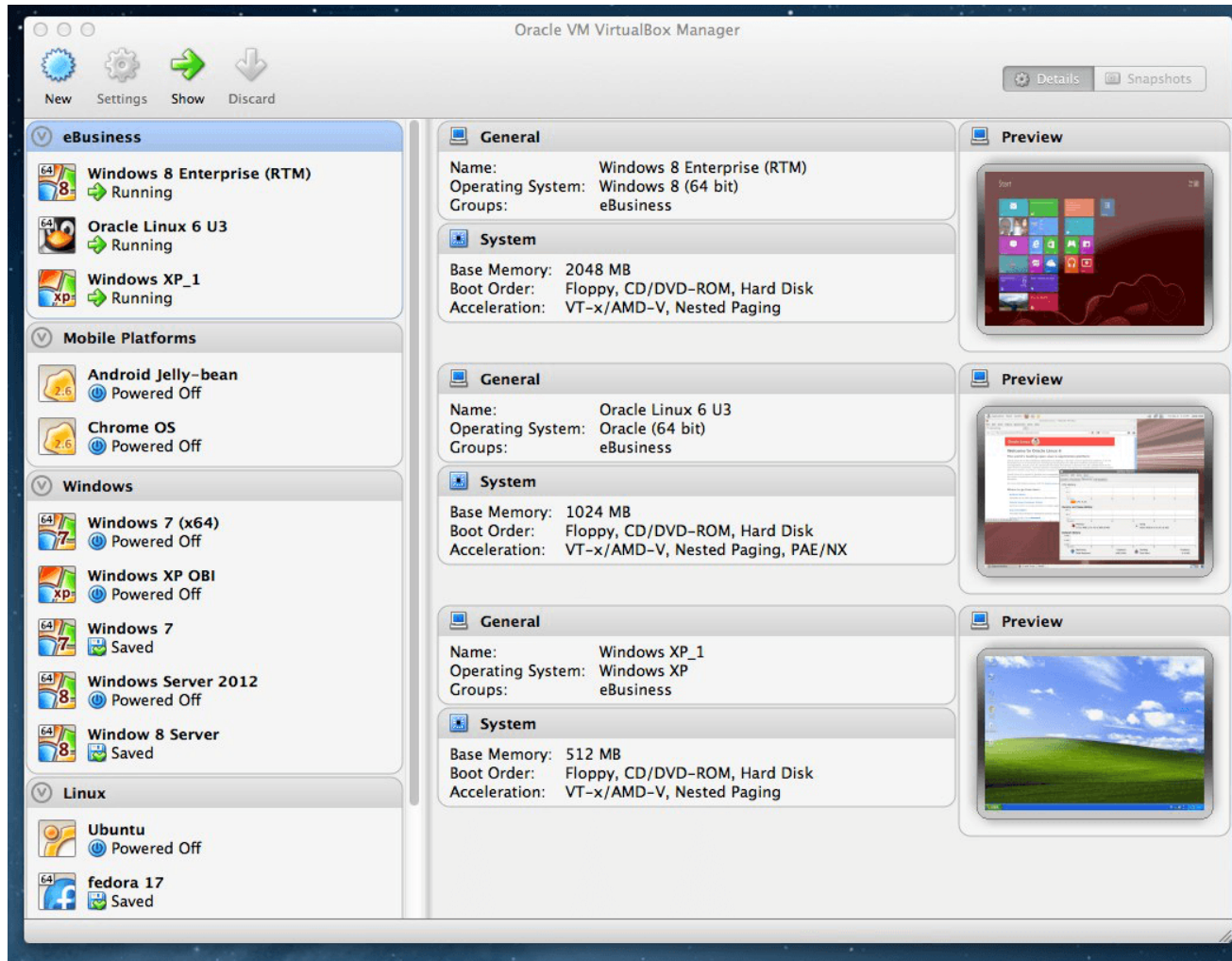
Virtualization with VirtualBox

- Terminology:
 - *Host OS*: the OS of the physical computer on which VirtualBox was installed
 - *Guest OS*: the OS that is running inside the VM
 - *Virtual machine (VM)*: special environment that VirtualBox creates for your guest OS while it is running
 - You run your guest OS “in” a VM
- VirtualBox files:
<https://www.virtualbox.org/wiki/Downloads>

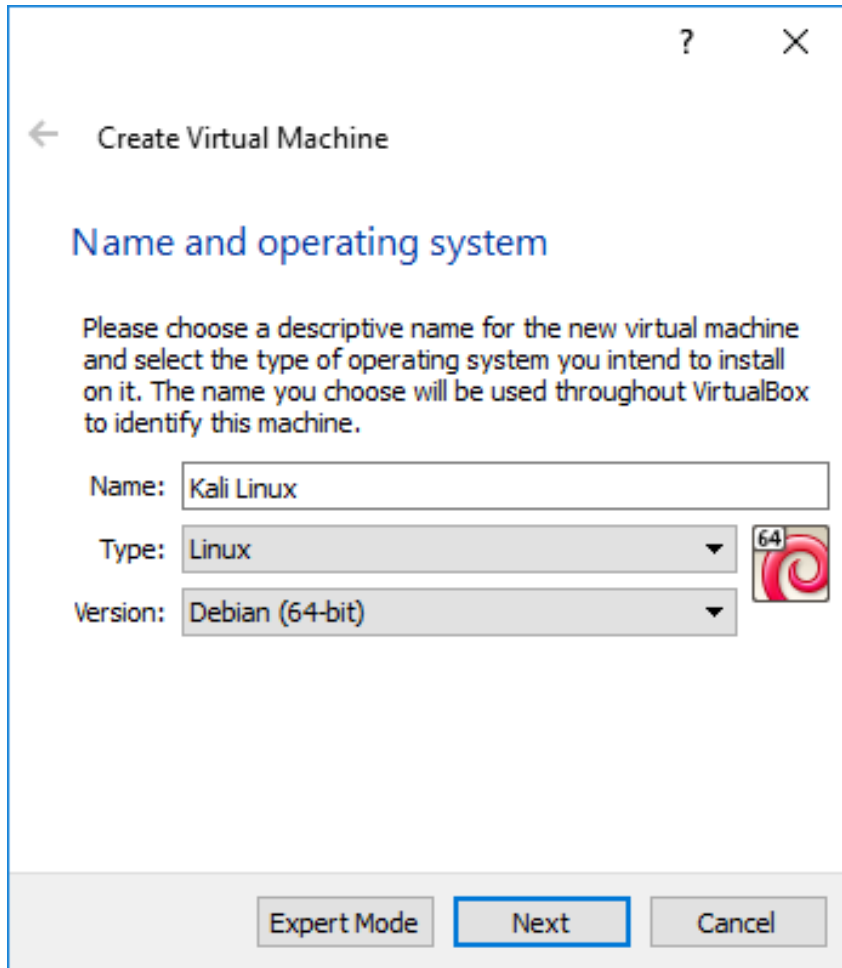
VirtualBox Installation

- Two additional VirtualBox installation steps:
 - To extend the functionality of the VirtualBox base package by adding extra features
 - Install ***VirtualBox Extension Pack***:
 - Extensions for Virtual USB 2.0 (EHCI) and USB 3.0 (xHCI) devices, VRDP support, host webcam passthrough, PCI passthrough, disk image encryption with AES, ...
 - Install ***Guest Additions***:
 - VirtualBox packages to be installed inside of a VM to improve the performance of the guest OS
 - Extensions for Mouse pointer integration, shared folders, shared clipboard, ...

VirtualBox: Main Interface



VirtualBox & Kali Installation




← Create Virtual Machine

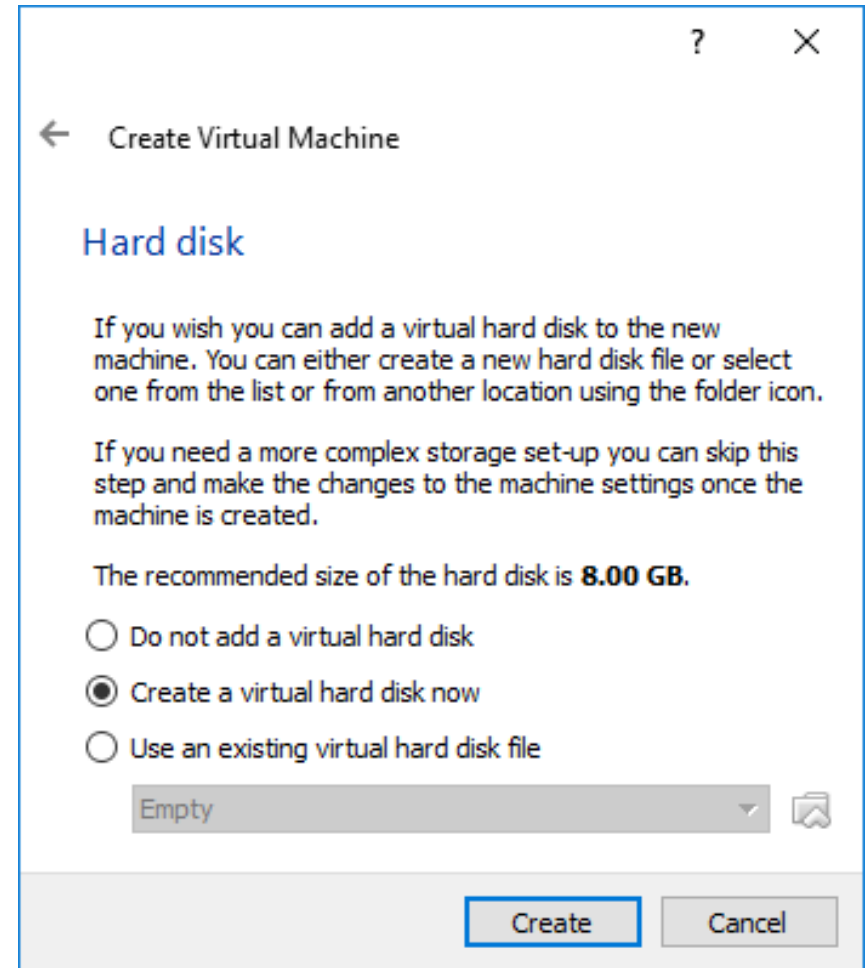
Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type: 

Version:



← Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.


If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

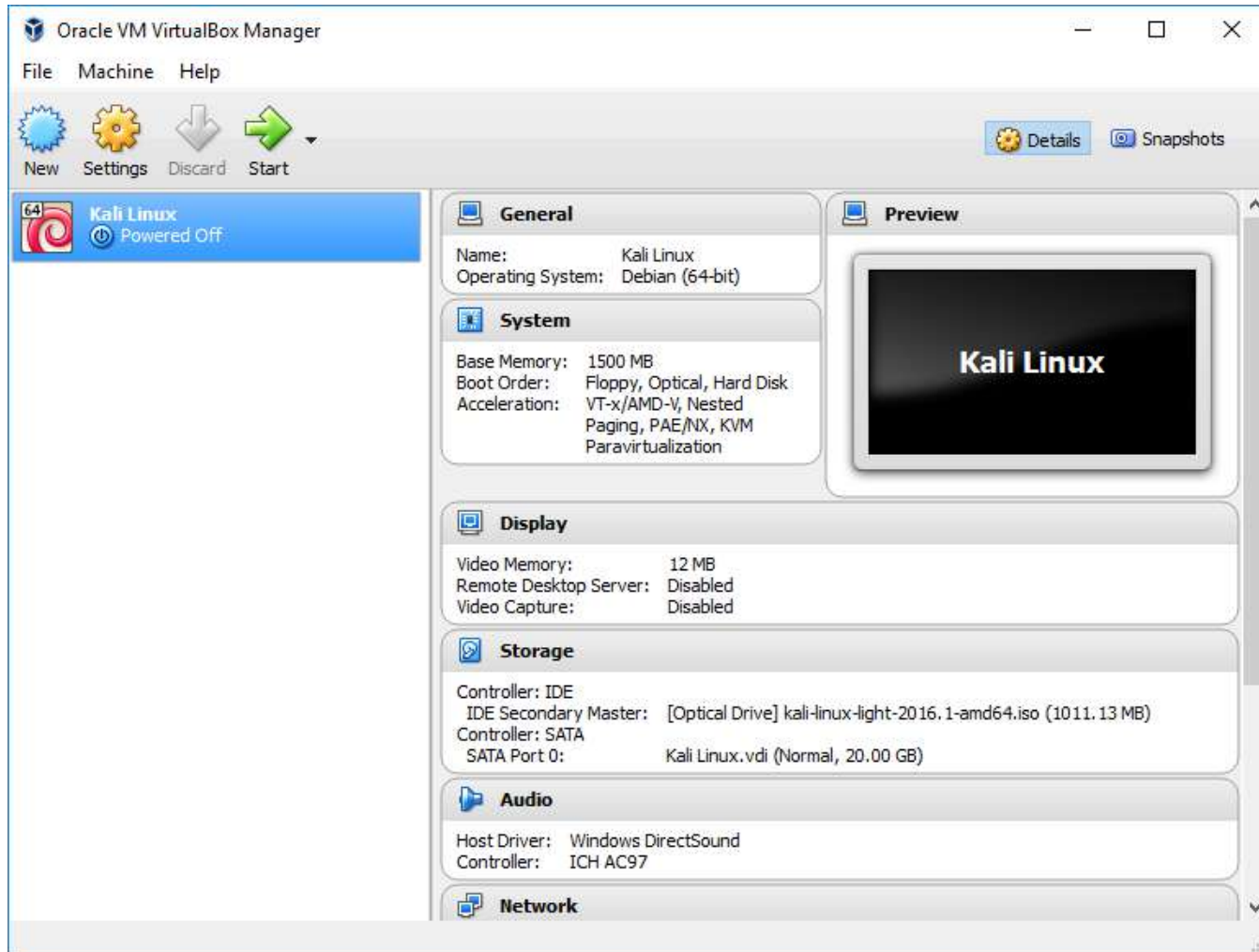
☐ Do not add a virtual hard disk

☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file

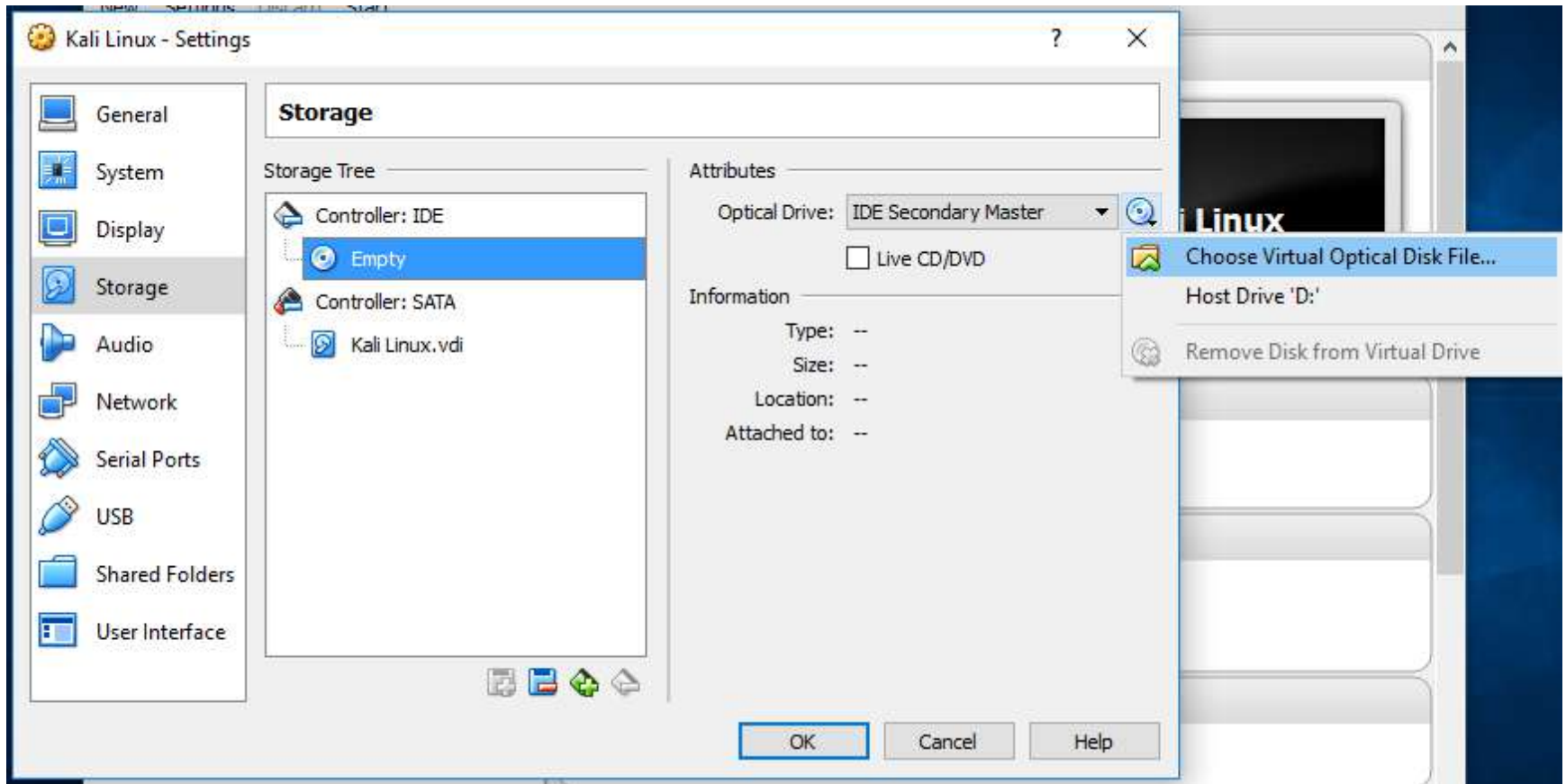


VirtualBox & Kali Installation



Source: “Kali Linux Revealed”, Hertzog et al., 2017

VirtualBox & Kali Installation



VirtualBox & Kali Installation



VirtualBox & Virtual Appliances

- VirtualBox can also import/export VMs in the industry-standard **Open Virtualization Format (OVF)**
- *Virtual appliances*: disk images packaged together with configuration settings for easy distribution
- Appliances in OVF format can appear in 2 variants:
 - Several files (as one or several disk images) typically in VDI/VMDK/... format, and a textual description file in an XML dialect with an **.ovf extension**
 - Alternatively, the above files can be packed together into a single archive file, typically with an **.ova extension**

VirtualBox Host Key

- **Host key:** right Control key (Windows), left Command key (Mac)



Source: "Oracle VirtualBox User Manual", 2018

- **Usage** of host key:
 - To release mouse and keyboard ownership from the VM
 - To send special key combinations:
host key + Del to send Ctrl+Alt+Del
 - To resize the machine's window:
e.g. to enable and leave scale mode: *host key* + C

Networking in VirtualBox

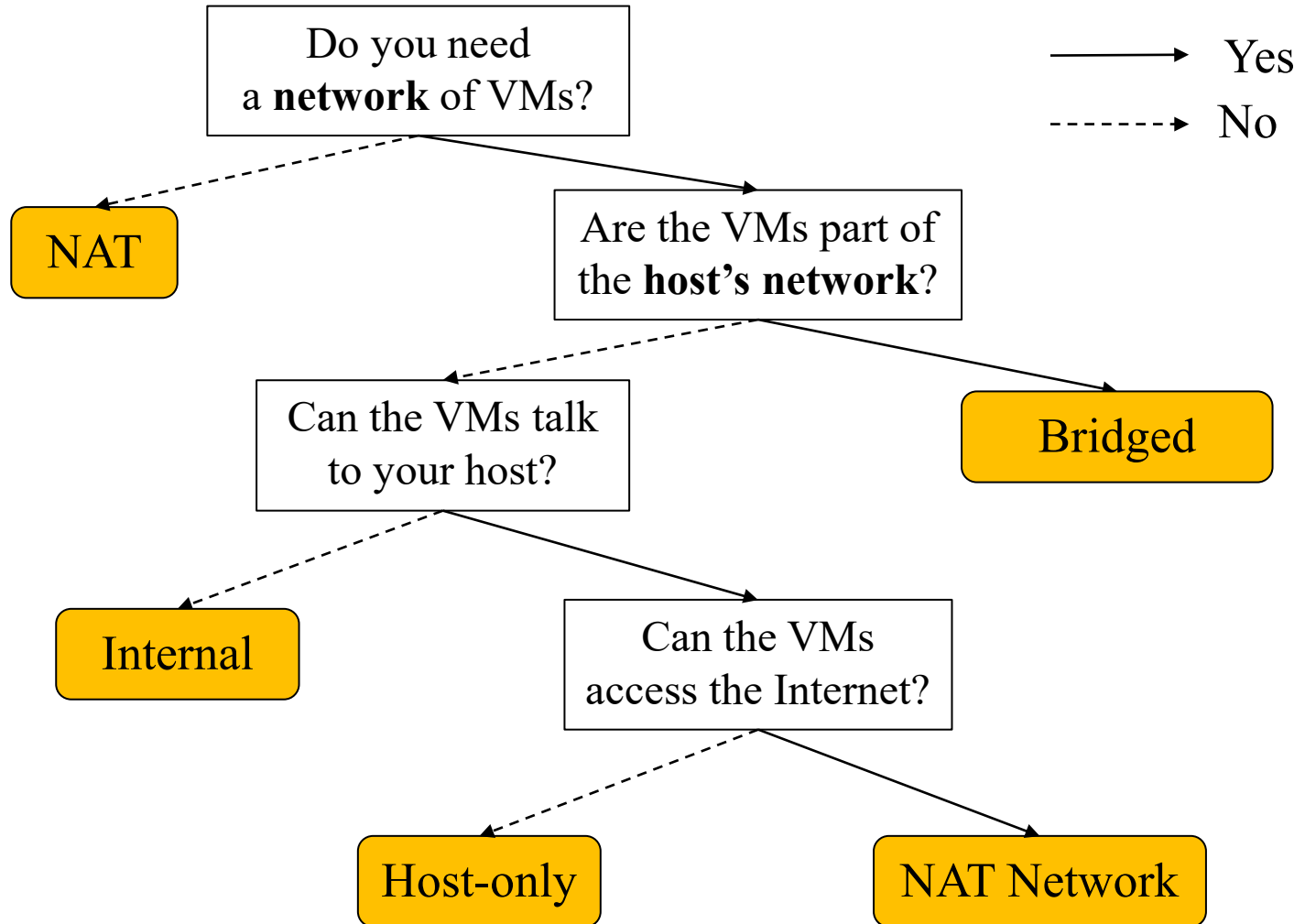
- Section 6 of VirtualBox User Manual 2020
- Various networking modes in VirtualBox:

| Mode | VM→Host | VM←Host | VM1↔VM2 | VM→Net/LAN | VM←Net/LAN |
|------------|---------|--------------|---------|------------|--------------|
| Host-only | + | + | + | – | – |
| Internal | – | – | + | – | – |
| Bridged | + | + | + | + | + |
| NAT | + | Port forward | – | + | Port forward |
| NATservice | + | Port forward | + | + | Port forward |

Source: “Oracle VirtualBox User Manual”, 2020

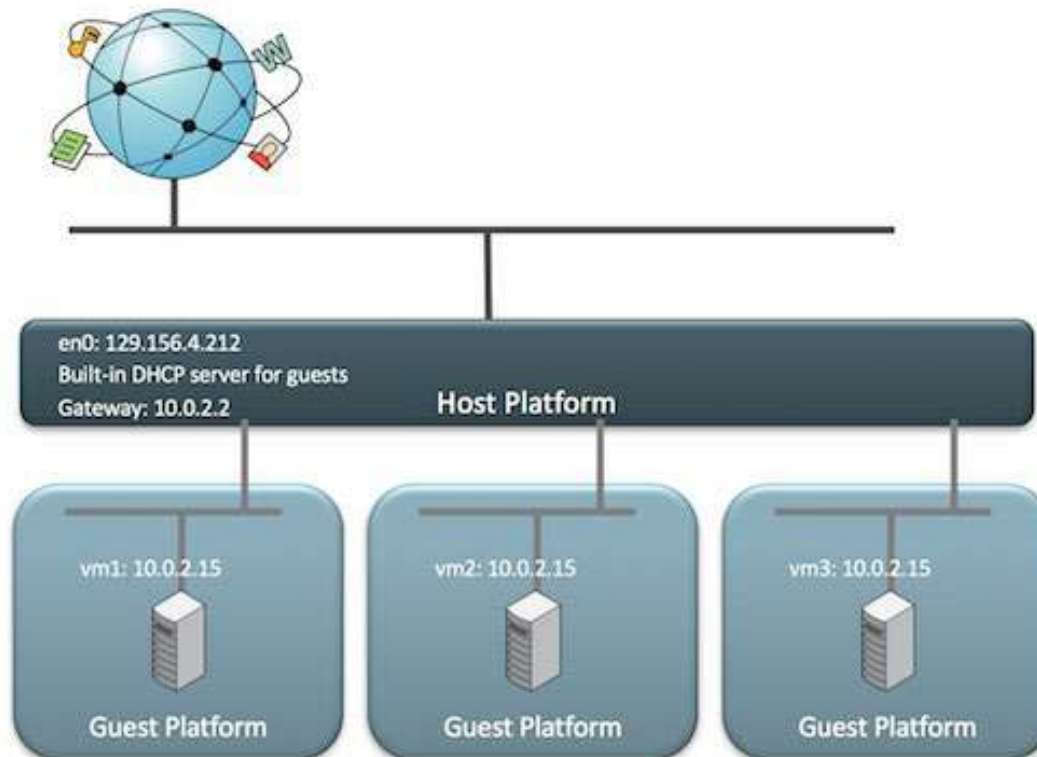
- *Question:* How do you choose a suitable networking mode for your need?

Networking in VirtualBox: Selection



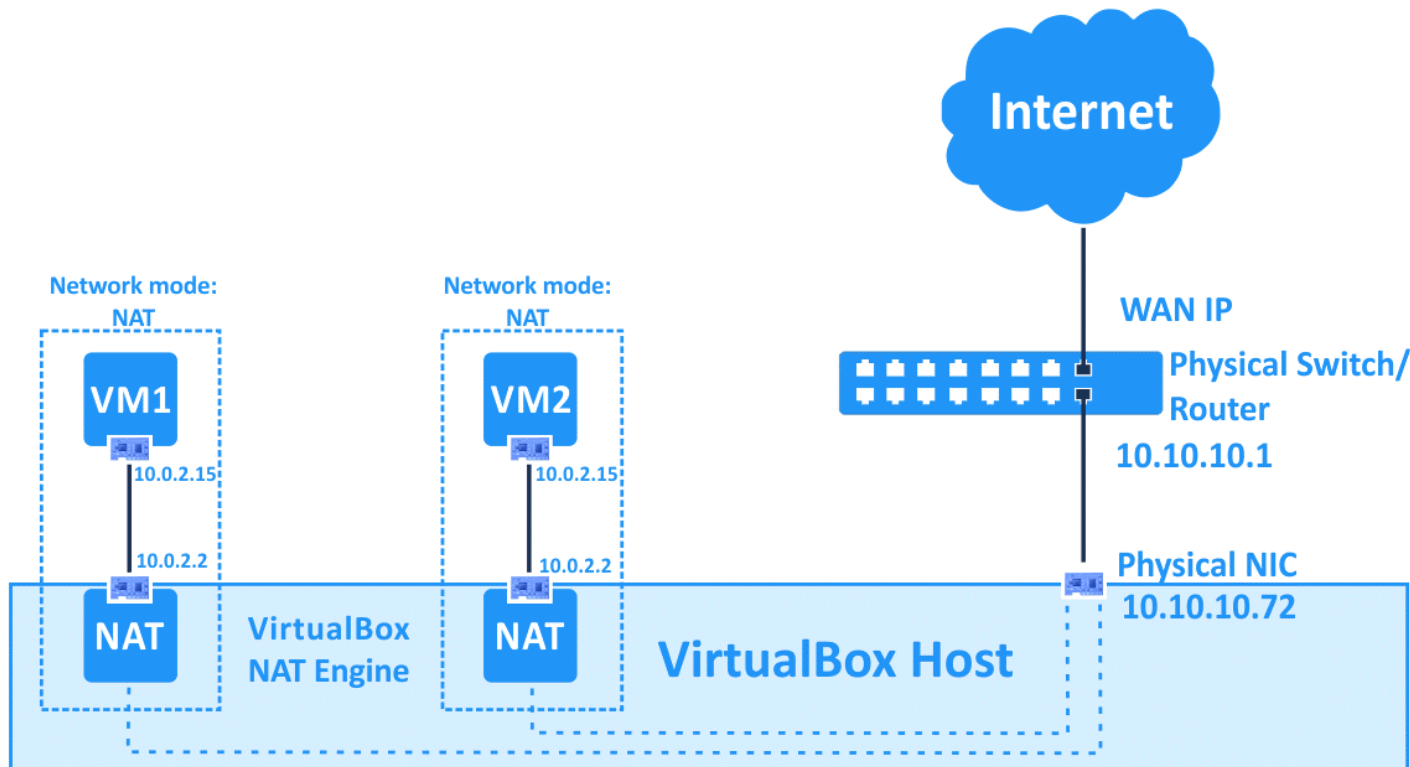
Additional Explanation: Illustration

- See: <https://blogs.oracle.com/scoter/networking-in-virtualbox-v2>
- **NAT mode:**



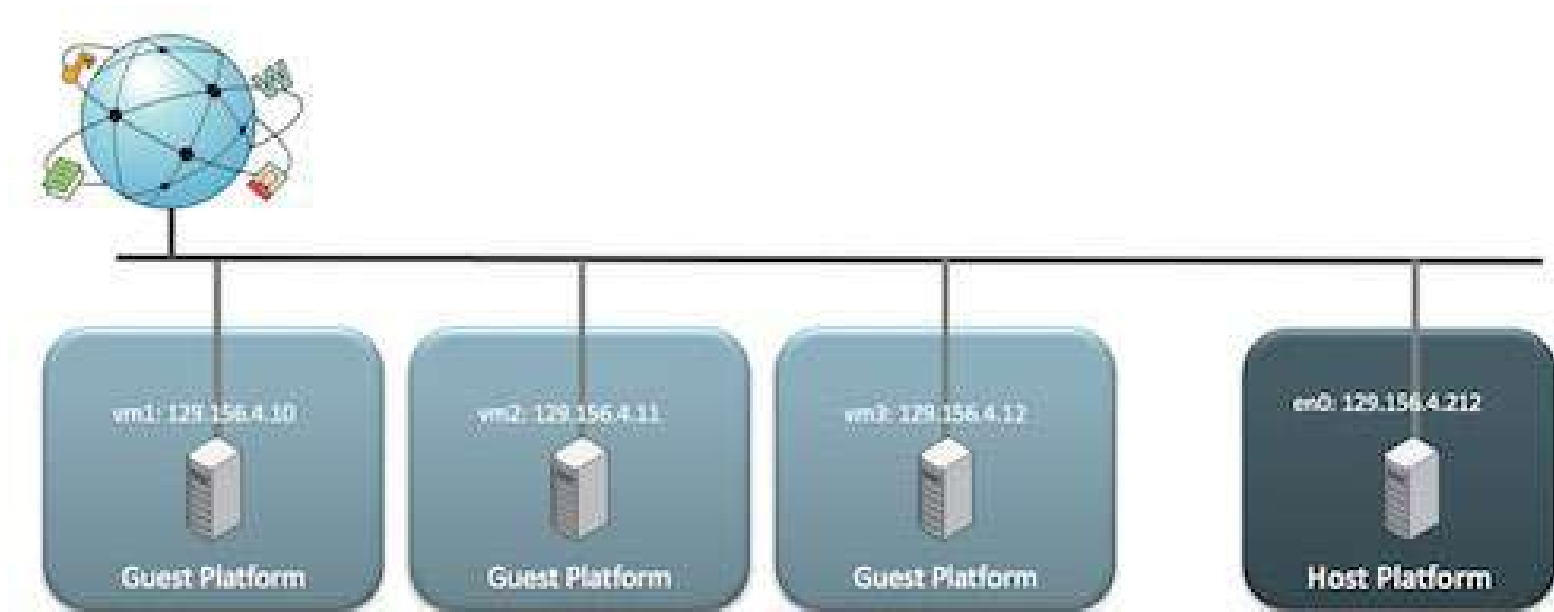
Additional Explanation: Illustration

- See: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>
- **NAT mode:**



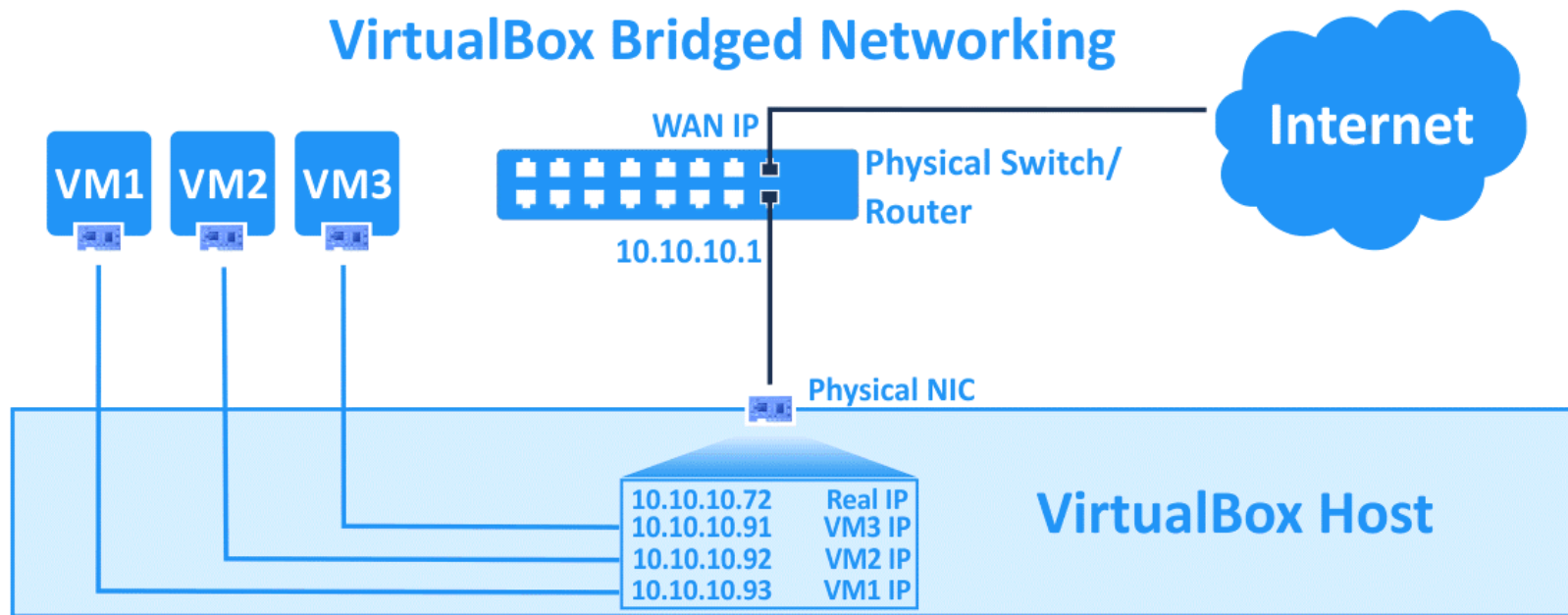
Additional Explanation: Illustration

- See: <https://blogs.oracle.com/scoter/networking-in-virtualbox-v2>
- **Bridged mode:**



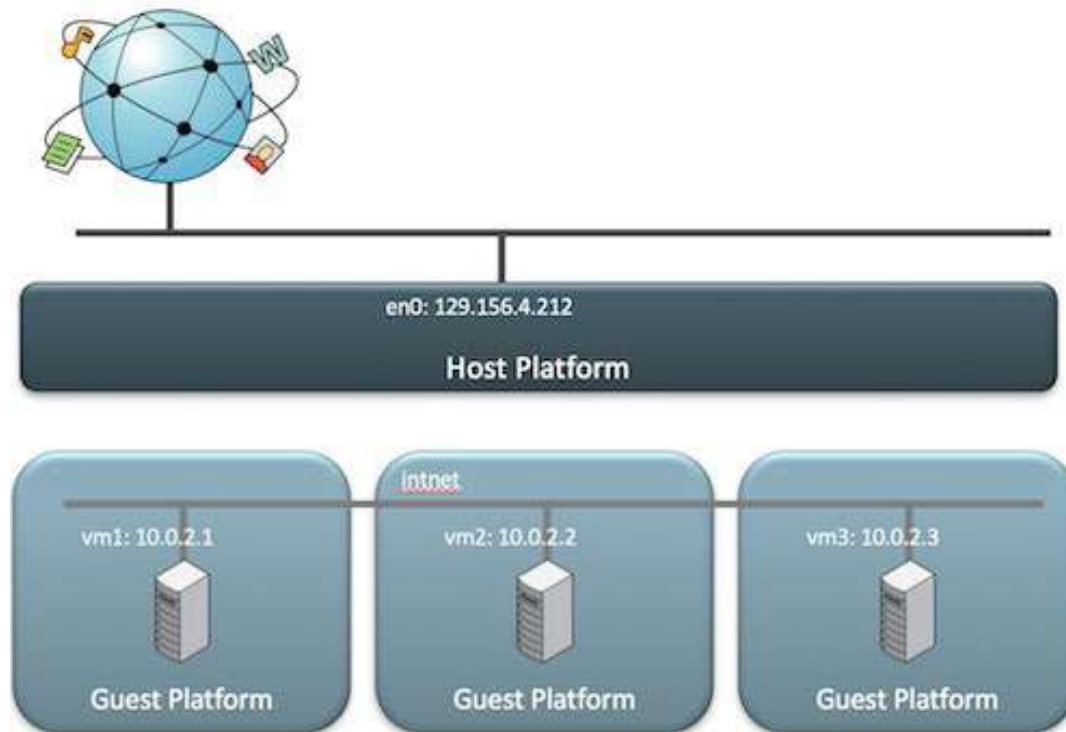
Additional Explanation: Illustration

- See: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>
- **Bridged mode:**



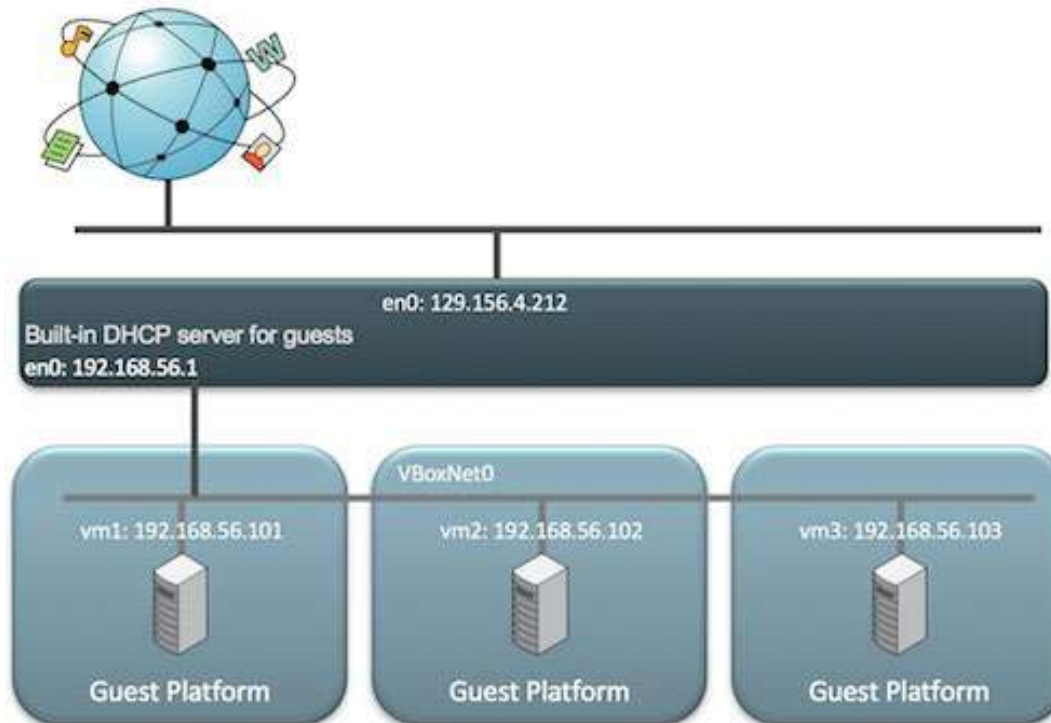
Additional Explanation: Illustration

- See: <https://blogs.oracle.com/scoter/networking-in-virtualbox-v2>
- **Internal** mode:



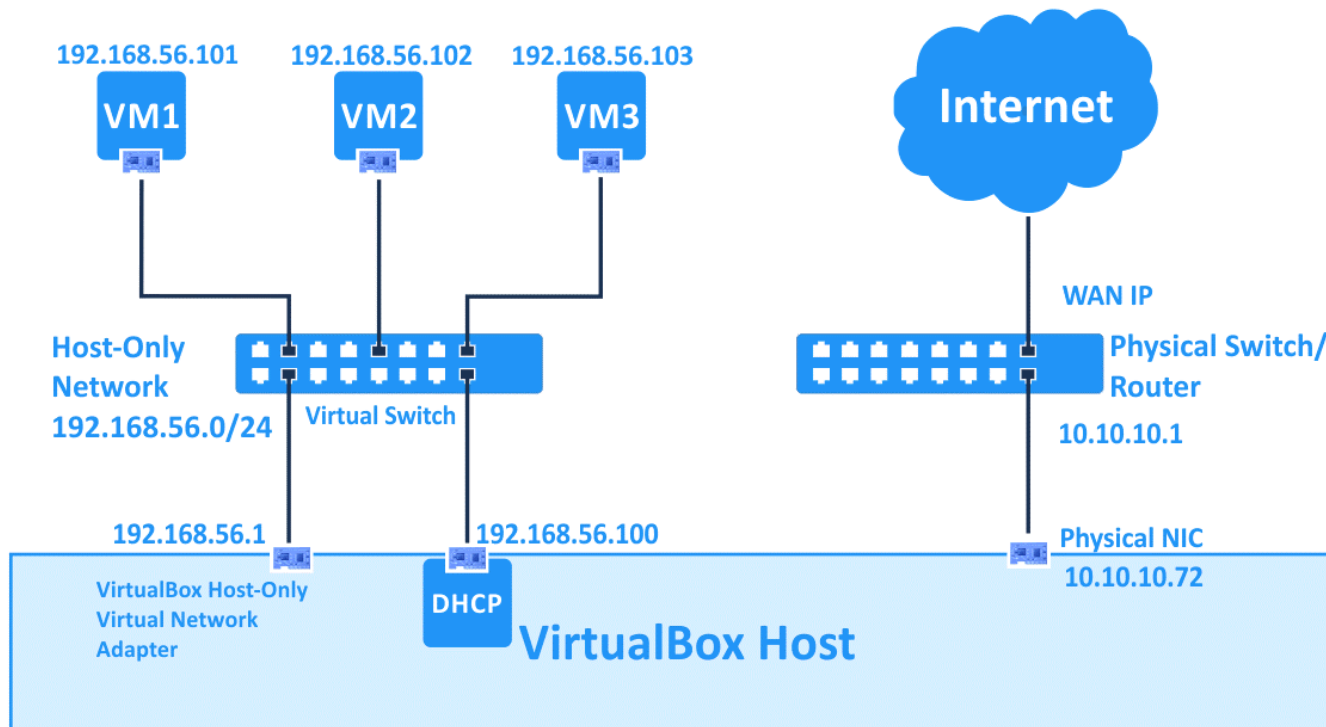
Additional Explanation: Illustration

- See: <https://blogs.oracle.com/scoter/networking-in-virtualbox-v2>
- **Host-only** mode:



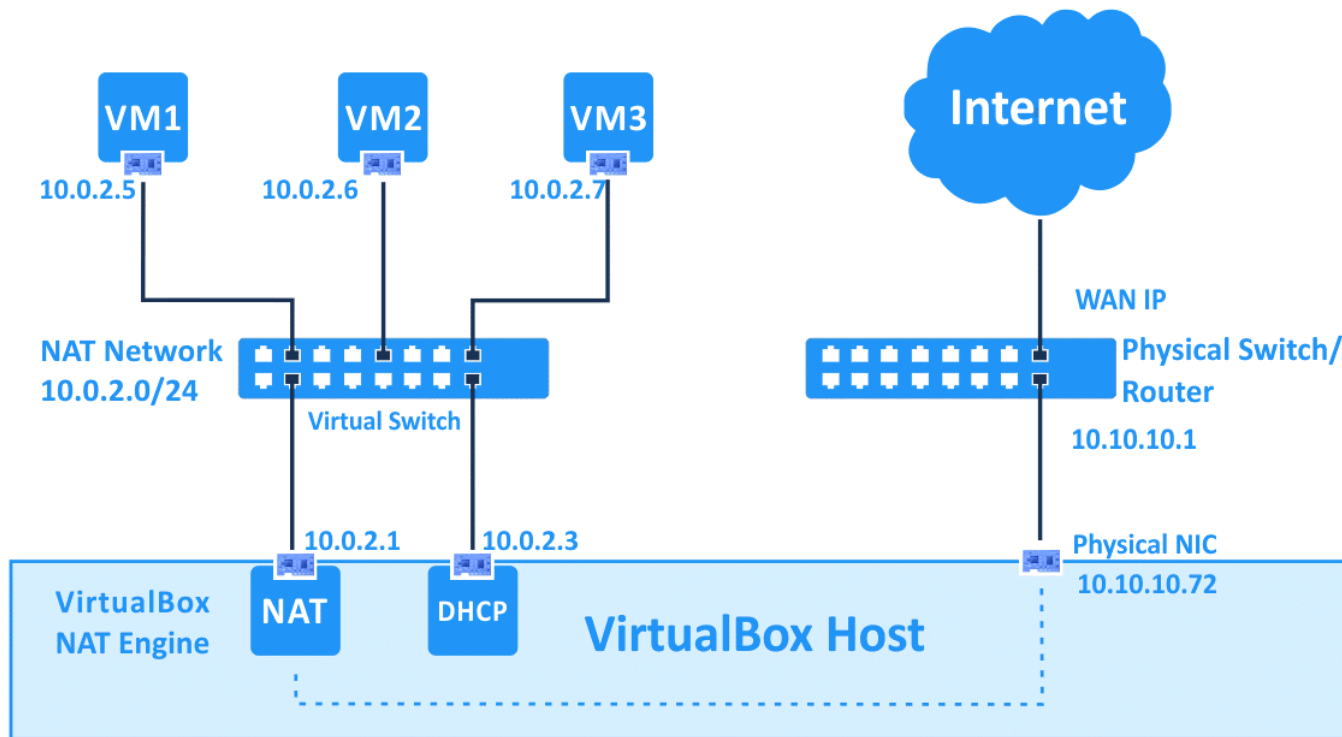
Additional Explanation: Illustration

- See: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>
- **Host-only mode:**



Additional Explanation: Illustration

- See: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>
- **NAT network** mode:



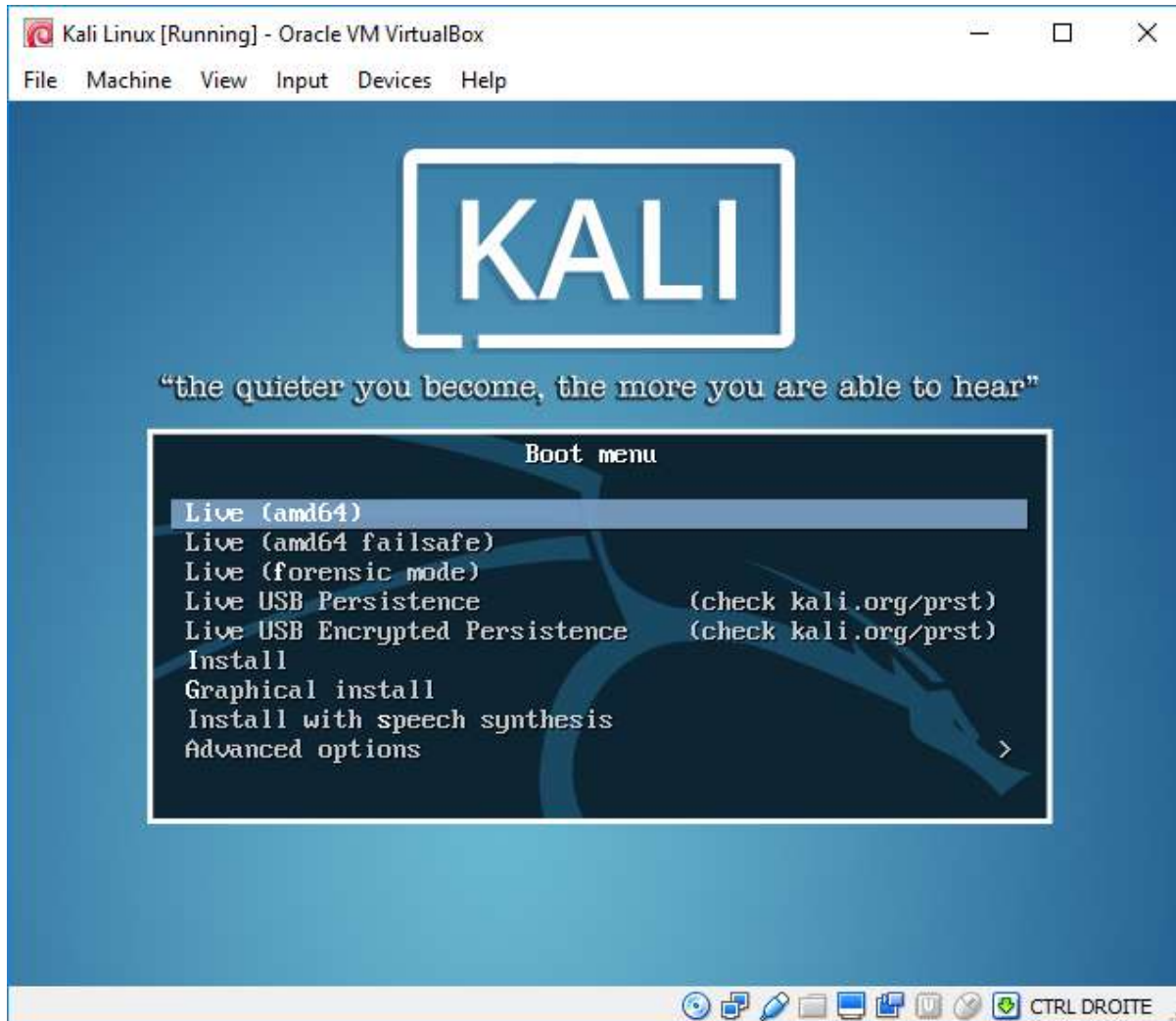
Kali Linux

Kali Linux



- What is Kali Linux?
 - Debian-based Linux distribution
 - Aimed at *penetration testing* and also *security auditing* (e.g. computer forensics, reverse engineering)
 - Maintained by Offensive Security
 - A rebuild of BackTrack Linux
 - First released in 2013
- Good documentation: “Kali Linux Revealed”, free e-book is available:
<https://www.kali.org/download-kali-linux-revealed-book/>

Kali Linux: Boot Menu



Source: "Kali Linux Revealed", Hertzog et al., 2017

Kali Linux & Pen-Testing

- Comes with >600 security tools pre-installed: nmap, Wireshark, Metasploit, John the Ripper, Burp Suite, ...
- “Single, root user” scenario: root/toor
- Network services disabled by default
- Can run within a virtual machine: e.g. VirtualBox
- Can utilize CPU’s virtualization features:
 - Enable “Intel® Virtualization Technology (VT)” and/or “Intel® VT-d Feature” options at the BIOS/UEFI setting

Kali Linux: Applications

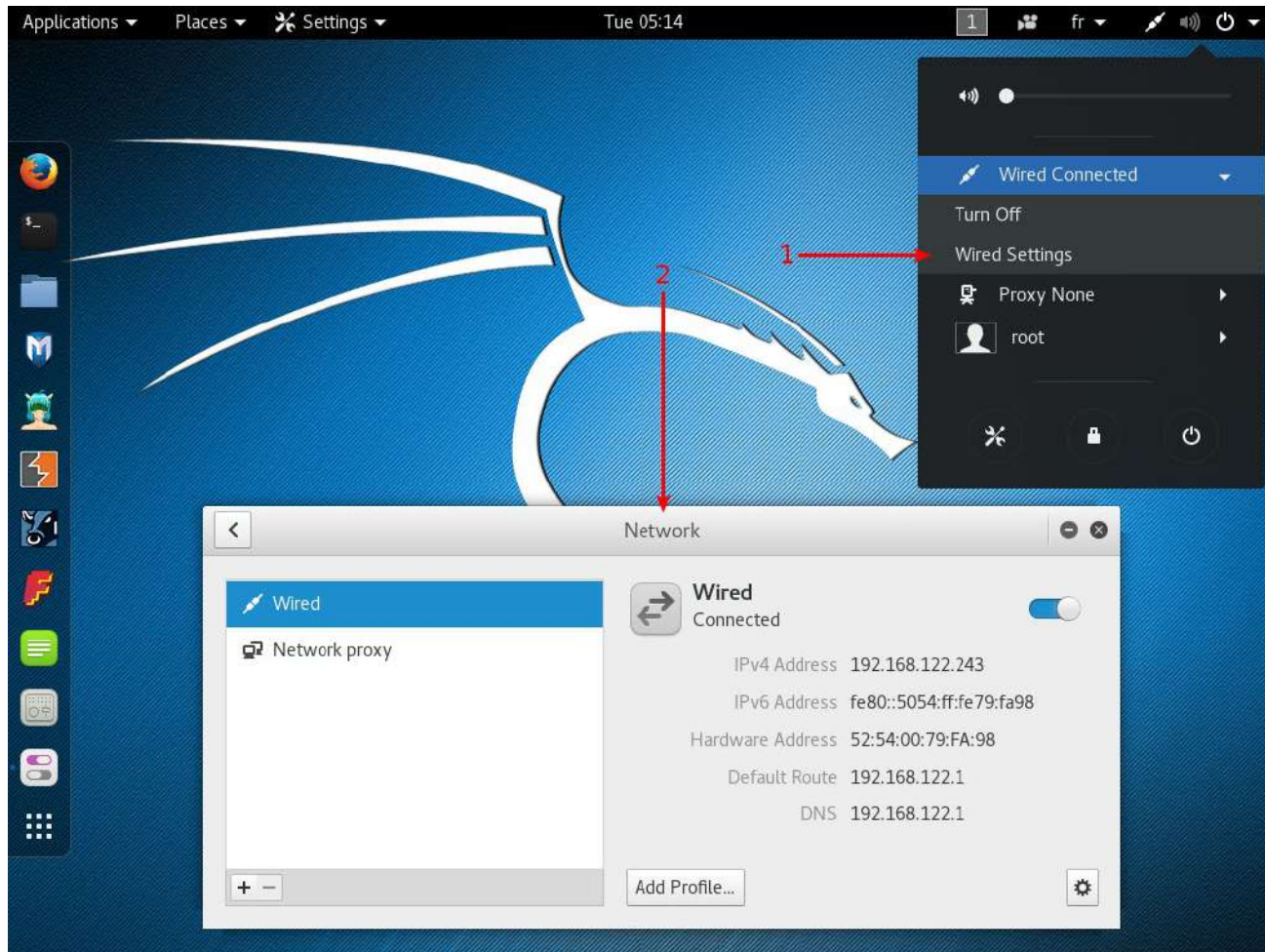


Kali Linux Version & Updating

- Check Linux and Kali versions:
 - `uname -a`: print system information
 - `lsb_release -a`: print distribution specific (Linux standard base) information
 - `cat /etc/*{release,version}`: OS release/version files
- Updating Kali Linux:
 - `apt-get update && apt-get upgrade`

Configuring Kali Linux: Network Setting

- *NetworkManager* setting interface:



Configuring Kali Linux: Network Setting

- Manual network setting steps:
 - `ifdown <network-device>`
 - **Modify** `/etc/network/interfaces`
 - `ifup <network-device>`
- **Setting** `/etc/network/interfaces` for a plain DHCP configuration:

```
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet dhcp
```

Configuring Kali Linux: Network Setting

- **Setting** `/etc/network/interfaces` for a static IP configuration:

```
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet static
address 192.168.0.3
netmask 255.255.255.0
broadcast 192.168.0.255
network 192.168.0.0
gateway 192.168.0.1
```

Configuring Kali Linux: Screen Setting

- Disabling blank screen:
 - Access “All Settings” → Power
 - Set “Blank screen” to *never*
- Disabling screen lock:
 - Access “All Settings” → Privacy
 - Set “Automatic Screen Lock” to *off*

Configuring Kali Linux: User & Group

- User management files:
 - List of users: `/etc/passwd`
 - Encrypted passwords of users: `/etc/shadow`
- Group management files:
 - List of groups: `/etc/group`
 - Encrypted passwords of groups: `/etc/gshadow`
- Some user-related commands:
 - `adduser`, `chfn`, `chsh`, `chage`
 - `passwd`, `passwd -e user`, `passwd -l user`

Configuring Kali Linux: Services

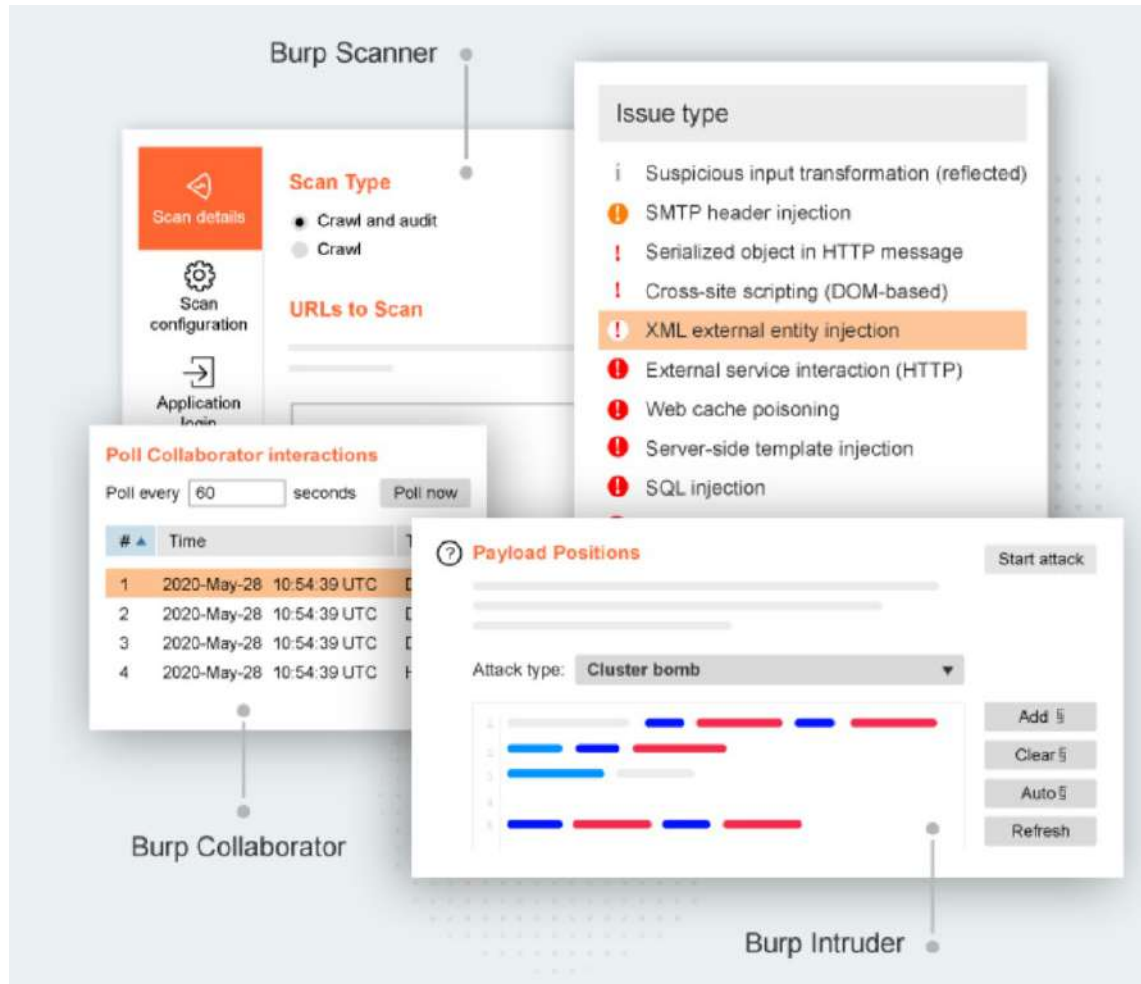
- Managing services:
 - E.g. ssh:
 - `systemctl start ssh`
 - `systemctl enable ssh`
 - `systemctl reload ssh`
 - E.g. Apache:
 - `systemctl start apache2`
 - `a2enmod module`
 - `a2dismod module`

Burp Suite

Burp Suite

- A very popular web pen-testing suite: recommended!
- You can install it:
 - On either your **Kali Linux** or **your host machine** (Windows, Linux, Mac)
 - As a **JAR file** (with Java required) or with **an installation process**
- Burp Suite versions:
 - **Community** edition: free
 - **Professional:**
 - 399 USD, free trial (for 30 days!)
 - Its features: <https://portswigger.net/burp/pro/features>

Burp Suite Professional



Source:
<https://portswigger.net/burp/pro/features>