CS4238: Computer Security Practice

Lecture 1-B: Linux/UNIX Overview

Slides by: LIANG Zhenkai, Roland YAP & SUFATRIO

Linux/UNIX Overview

(Chapter 3 of the reference book 1)

UNIX: A beautiful but strange beast

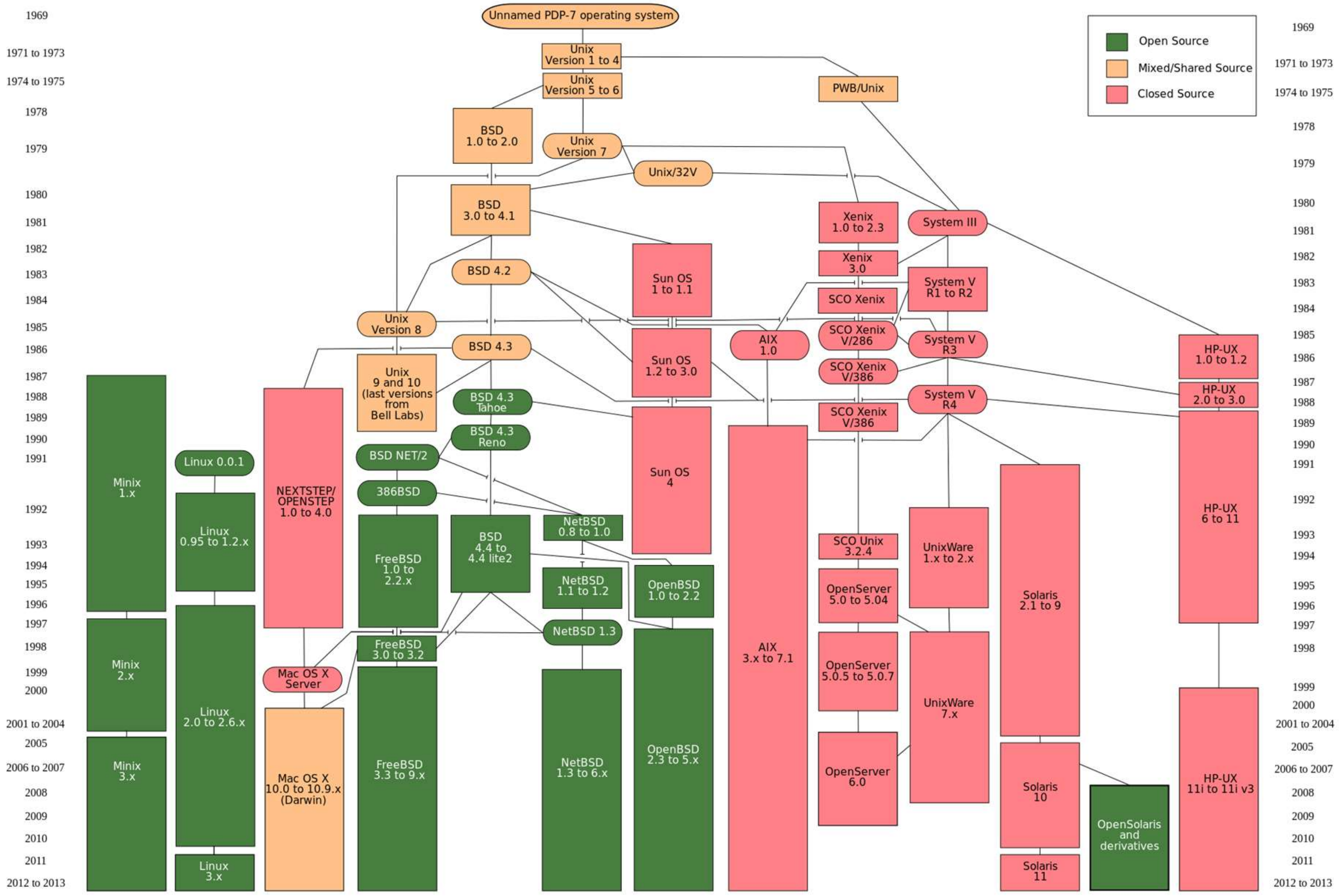
```
$ find . -name “abc” -exec rm {} \;
```

Unix philosophy: "**Swiss Army Knife**"

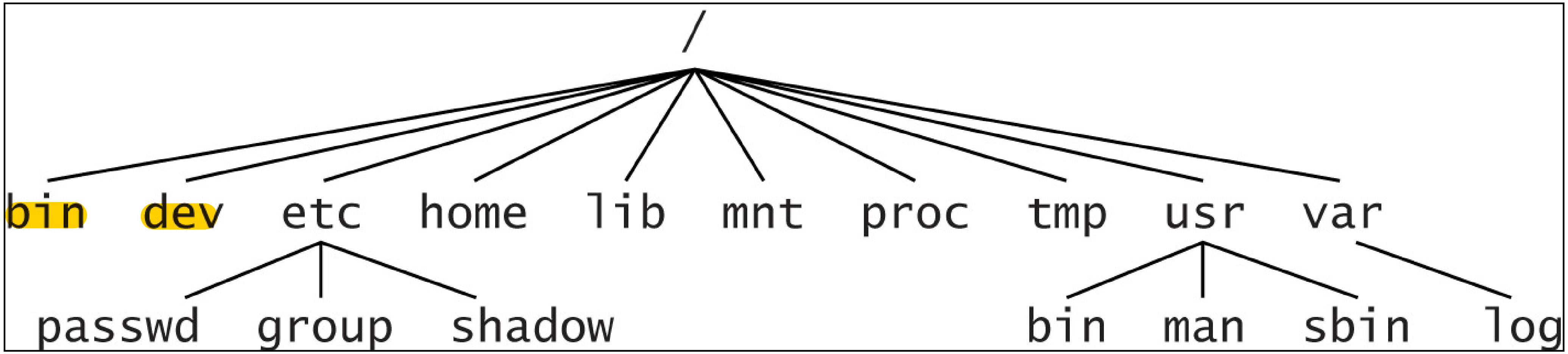
UNIX & Linux

- History from 1970s
- Many versions (Linux, Android, OSX + iOS, Solaris, AIX, ...)
- We will mainly use Linux
  - Open source (http://www.kernel.org)
  - (Relatively) easy to understand
    - Windows is closed source and full details are not well understood
  - Many tools (usually also open source)
  - Many distributions (we use Kali, Ubuntu)
    - Vary in setup, administration, kernel, ...

Simplified UNIX Family Tree



Linux File System Structure



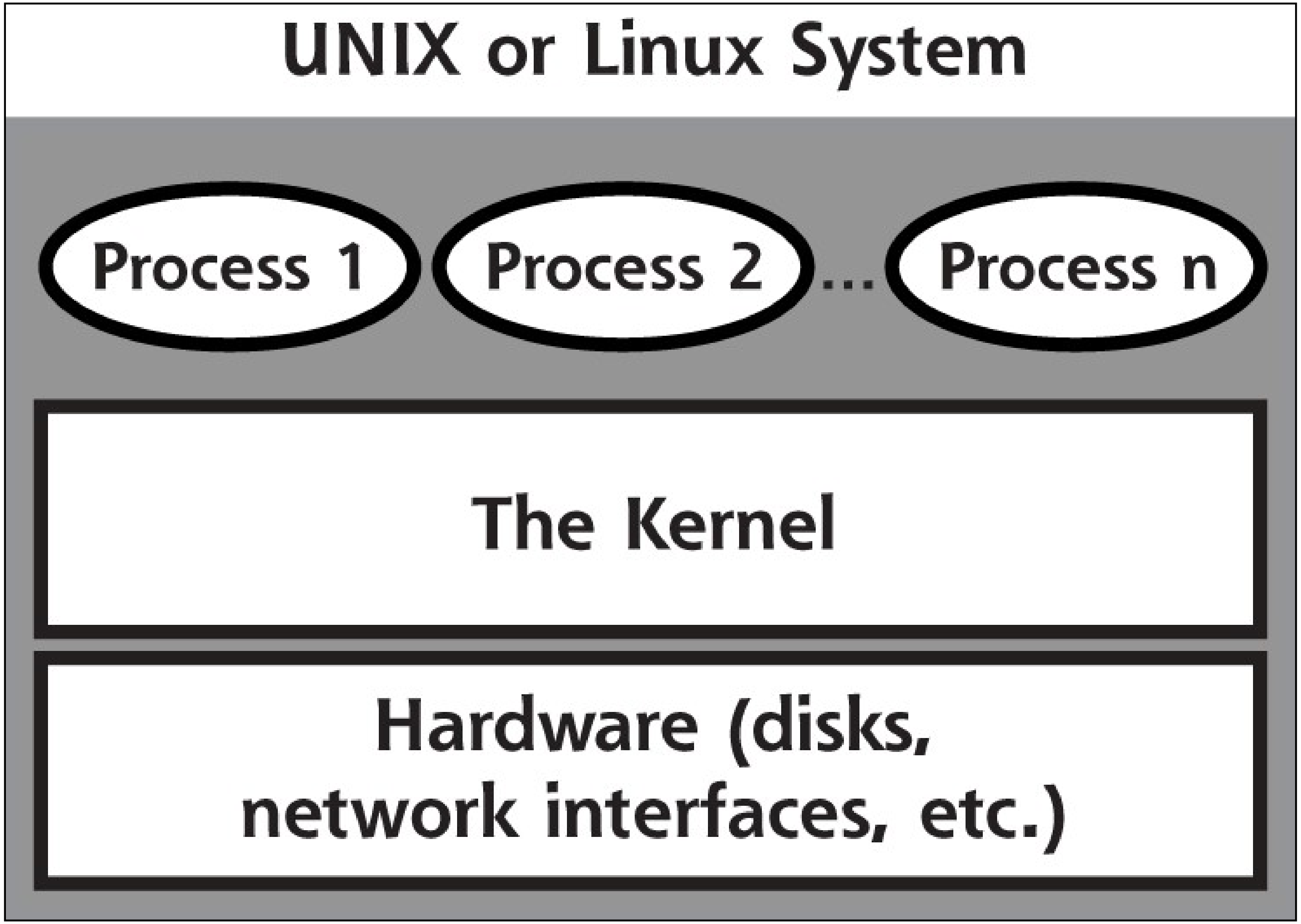
Source: Skoudis & Liston, Counter Hack Reloaded

```
/bin/ls

/etc/passwd

/home

/usr/bin

/var/log
```

Linux File System Structure

- Some notes:
  - Standard file system structure by convention
  - **Filesystem Hierarchy Standard (FHS)** from the Linux Foundation

Kernel and Processes



Source: Skoudis & Liston, Counter Hack Reloaded

Processes

talking about this for firewall

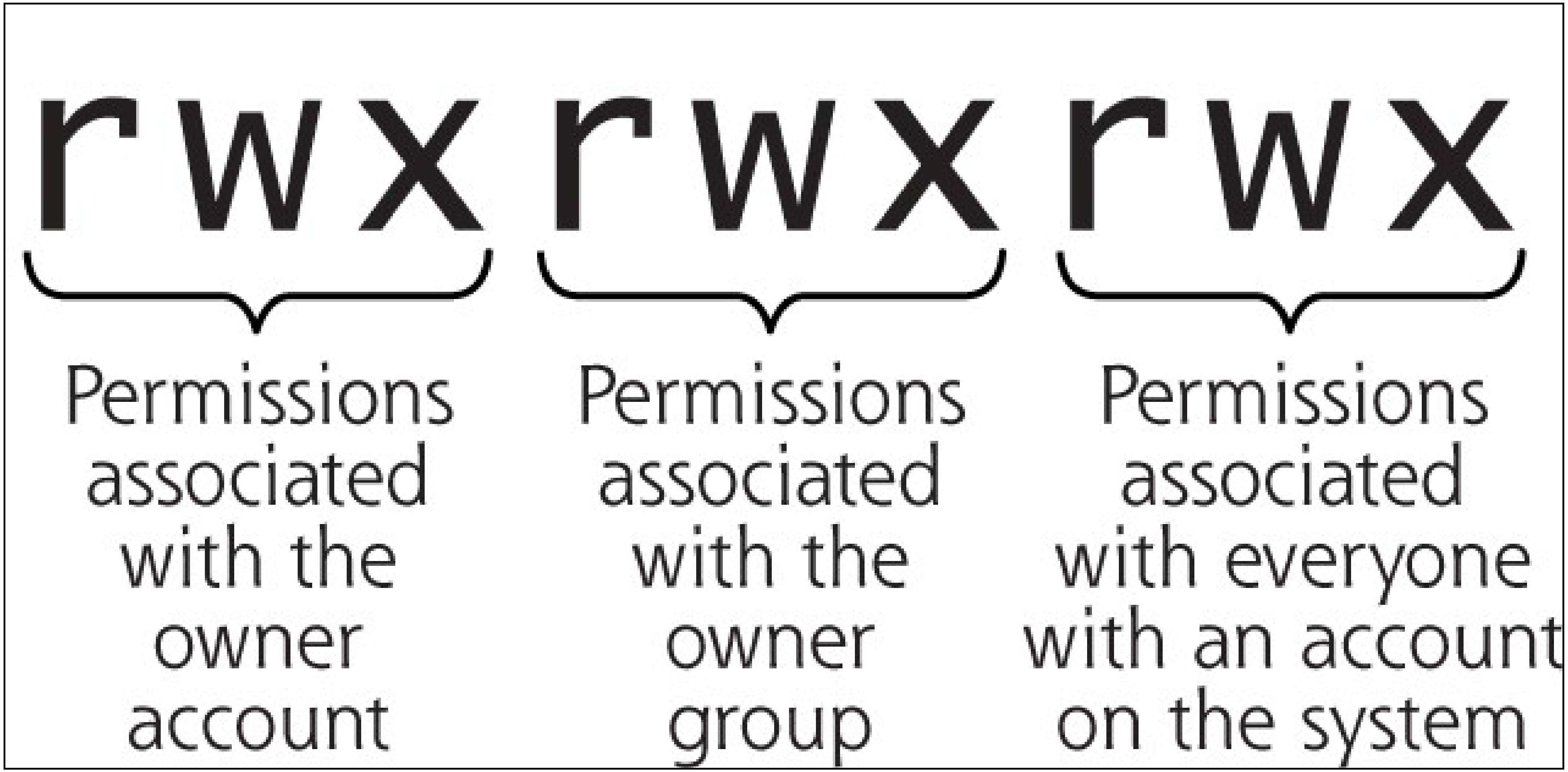
- Automatically starting up processes:
  - init, inetd, xinetd, cron
- Manually starting processes
- Analyzing processes:
  - ps command
  - lsof command (https://linux.die.net/man/8/lsof):
    - `lsof -p [pid], lsof -i, lsof +d|+D`

Accounts and Groups

- User database
  - `/etc/passwd`
  - `/etc/shadow`

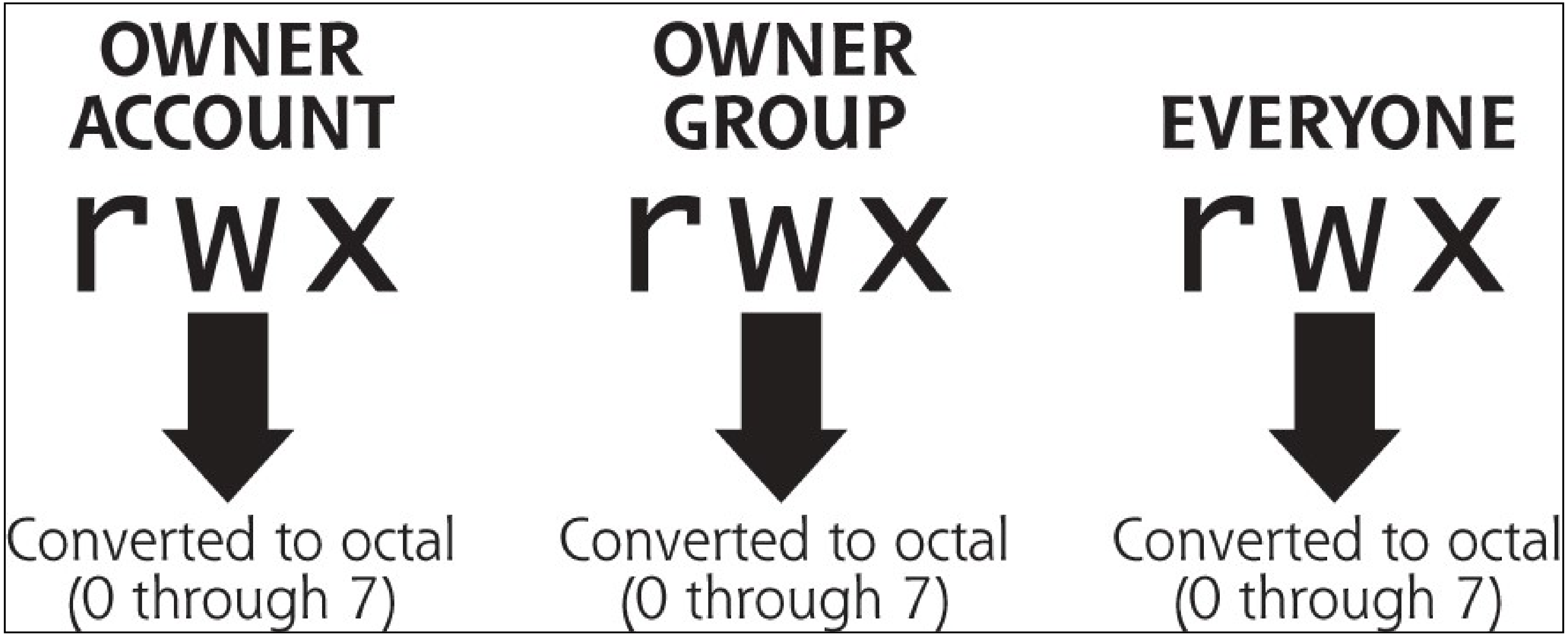
- Group database
  - `/etc/group`

File System Permissions


rwx rwx rwx
Permissions associated with the owner account
Permissions associated with the owner group
Permissions associated with everyone with an account on the system

Source: Skoudis & Liston, Counter Hack Reloaded

File System Permissions


OWNER ACCOUNT
rwx
Converted to octal (0 through 7)
OWNER GROUP
rwx
Converted to octal (0 through 7)
EVERYONE
rwx
Converted to octal (0 through 7)

Source: Skoudis & Liston, Counter Hack Reloaded

Setuid/Setgid Programs

- setuid/setgid bit
  - setuid: change user ID of a process to its file owner when executed (**passwd** example)
  - setgid: change user ID of process to its group owner when executed
  - Displayed as "s" permission bit
  - `# find / -uid 0 -perm -4000 -ls`
  - `# find / -perm -2000 -ls`
  - `# find / -perm /6000 -ls`

UNIX Manual Pages

- UNIX documentation using the **`man`** command
  - `man` is your friend!
  - Note: small variations in `man` with different UNIX

```
$ man ls
$ man man
```

- Organized into sections:
  - 1: Executable programs or shell commands
  - 2: System calls (functions provided by the kernel)
  - 3: Library calls (functions within program libraries)

UNIX Manual Pages

  - 4: Special files (usually found in /dev)
  - 5: File formats and conventions e.g. /etc/passwd
  - 6: Games
  - 7: Miscellaneous
  - …

- Examples:

```
$ man printf
$ man 1 printf
$ man 3 printf
```

Common Useful Commands

- Common UNIX programs:
  - `ls, ps, bash, kill, chmod, cp, rm, mkdir, rmdir, man, cat, less, logout, ssh, echo, wc, diff, who, grep, file, find, which, tty`
- Editors (console):
  - `vi, vim, emacs, pico`
- Bash shell commands:
  - `jobs, kill, fg, bg, cd, pwd, echo, exit`
- Free good resource to learning Linux commands:
  - W. Shotts, “The Linux Command Line”, `http://linuxcommand.org`

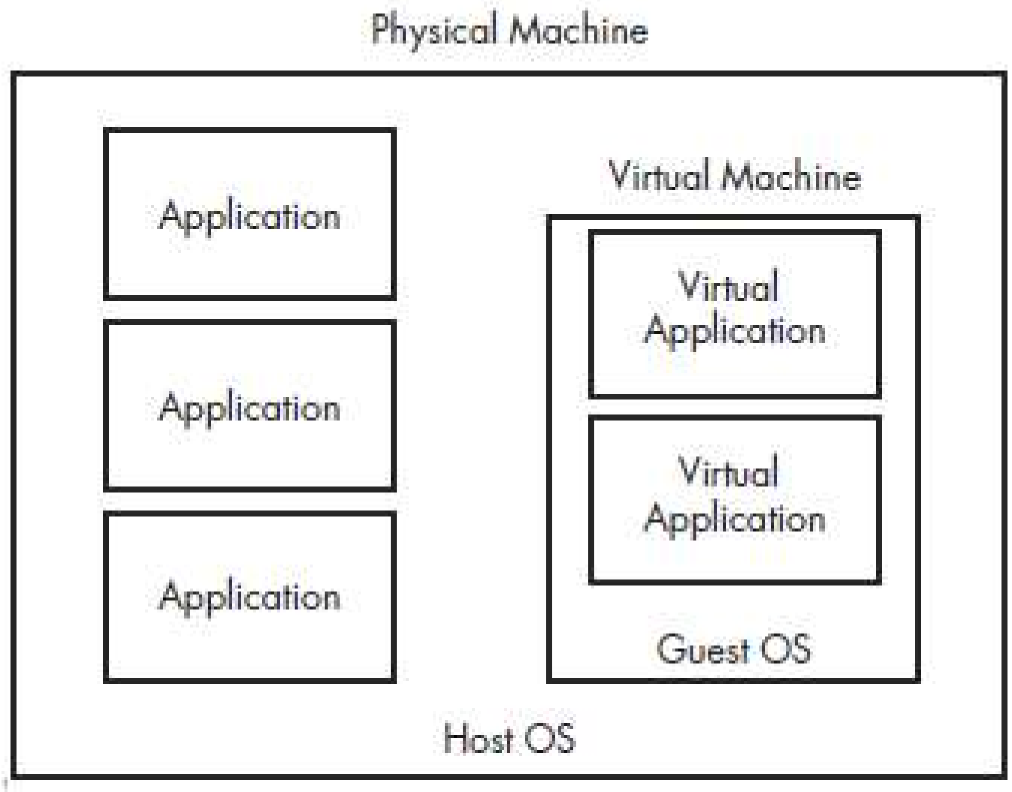
Ubuntu System

- Ubuntu desktop with Unity desktop environment

- Software installation
- Package management:
  - High-level command: `apt-get`
  - Low-level command: `dpkg` (`--list`, `--search`, `--status`)
- Network and service configuration: *next week*
- Some tips on Ubuntu's screen setting:
  - Disable blank screen & screen lock
  - Enable workspaces

Virtualization with VirtualBox

VM Illustration



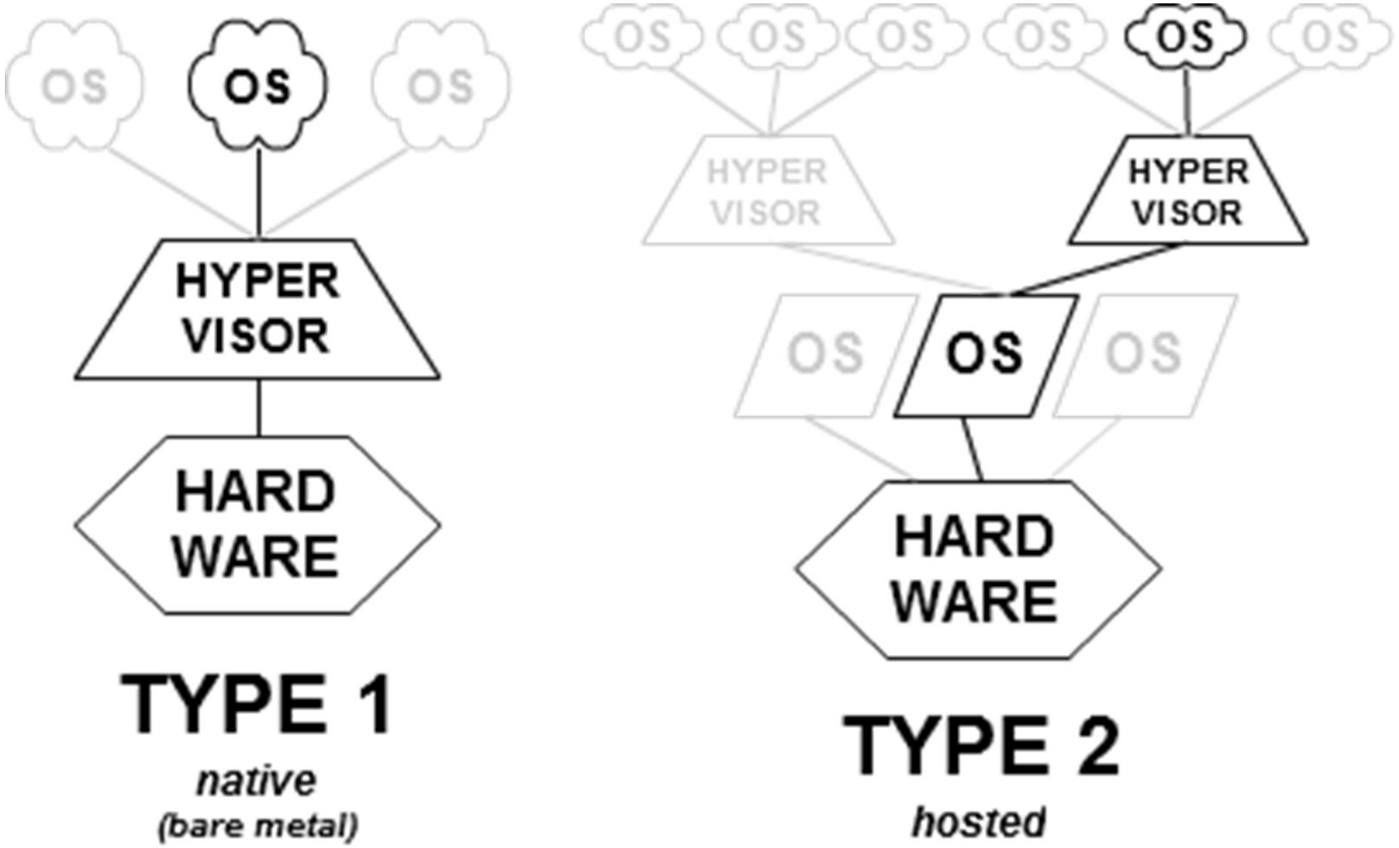
Source: Practical Malware Analysis

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`

Virtualization

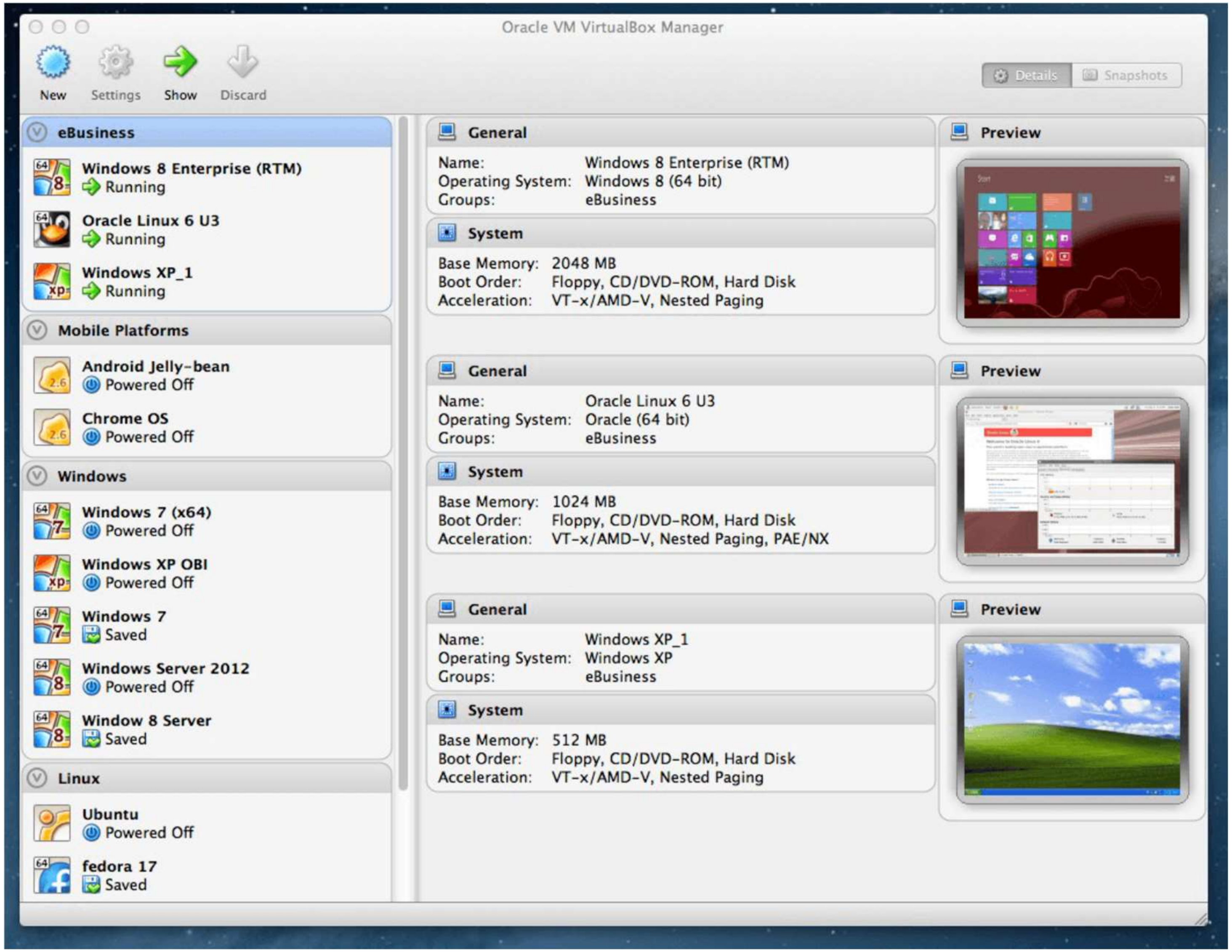


Source: Wikipedia

VirtualBox Installation

- Two additional VirtualBox installation steps:
  - Extend the functionality of the VirtualBox base package by adding extra features
  - Install ***VirtualBox Extension Pack***: Extend with:
    - 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 a VM to improve performance of the guest OS and to add extra features:
    - Mouse pointer integration, shared folders, shared clipboard, ...

VirtualBox: Main Interface



Oracle VM VirtualBox Manager

eBusiness

Windows 8 Enterprise (RTM)
Running

Oracle Linux 6 U3
Running

Windows XP_1
Running

Mobile Platforms

Android Jelly-bean
Powered Off

Chrome OS
Powered Off

Windows

Windows 7 (x64)
Powered Off

Windows XP OBI
Powered Off

Windows 7
Saved

Windows Server 2012
Powered Off

Window 8 Server
Saved

Linux

Ubuntu
Powered Off

fedora 17
Saved

General

Name: Windows 8 Enterprise (RTM)
Operating System: Windows 8 (64 bit)
Groups: eBusiness

System

Base Memory: 2048 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Preview

General

Name: Oracle Linux 6 U3
Operating System: Oracle (64 bit)
Groups: eBusiness

System

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Preview

General

Name: Windows XP_1
Operating System: Windows XP
Groups: eBusiness

System

Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Preview

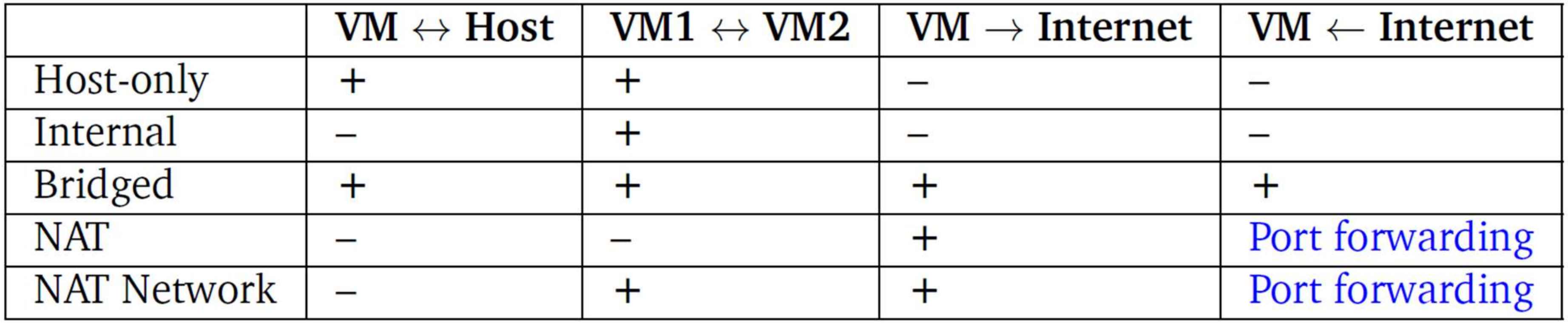
Source: “Oracle VirtualBox User Manual”, 2018

VirtualBox & Virtual Appliances

- VirtualBox can 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

Networking in VirtualBox

- Various networking modes in VirtualBox:



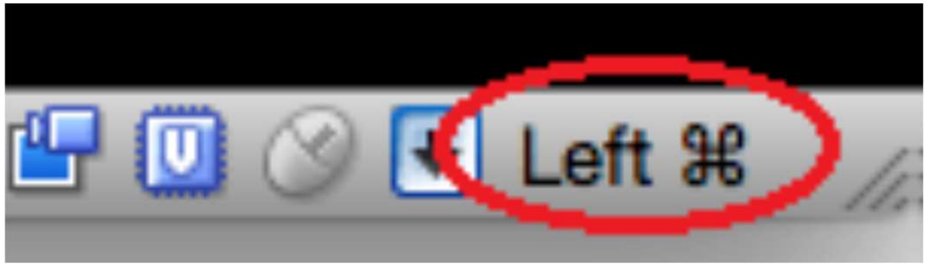
	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Host-only	+	+	–	–
Internal	–	+	–	–
Bridged	+	+	+	+
NAT	–	–	+	Port forwarding
NAT Network	–	+	+	Port forwarding

Source: “Oracle VirtualBox User Manual”, 2018

- *Question*: How do you choose a suitable networking mode for your need?
- *Answer*: To be discussed in *next lab*!

VirtualBox Host Key

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



Source: "Oracle VirtualBox User Manual", 2018

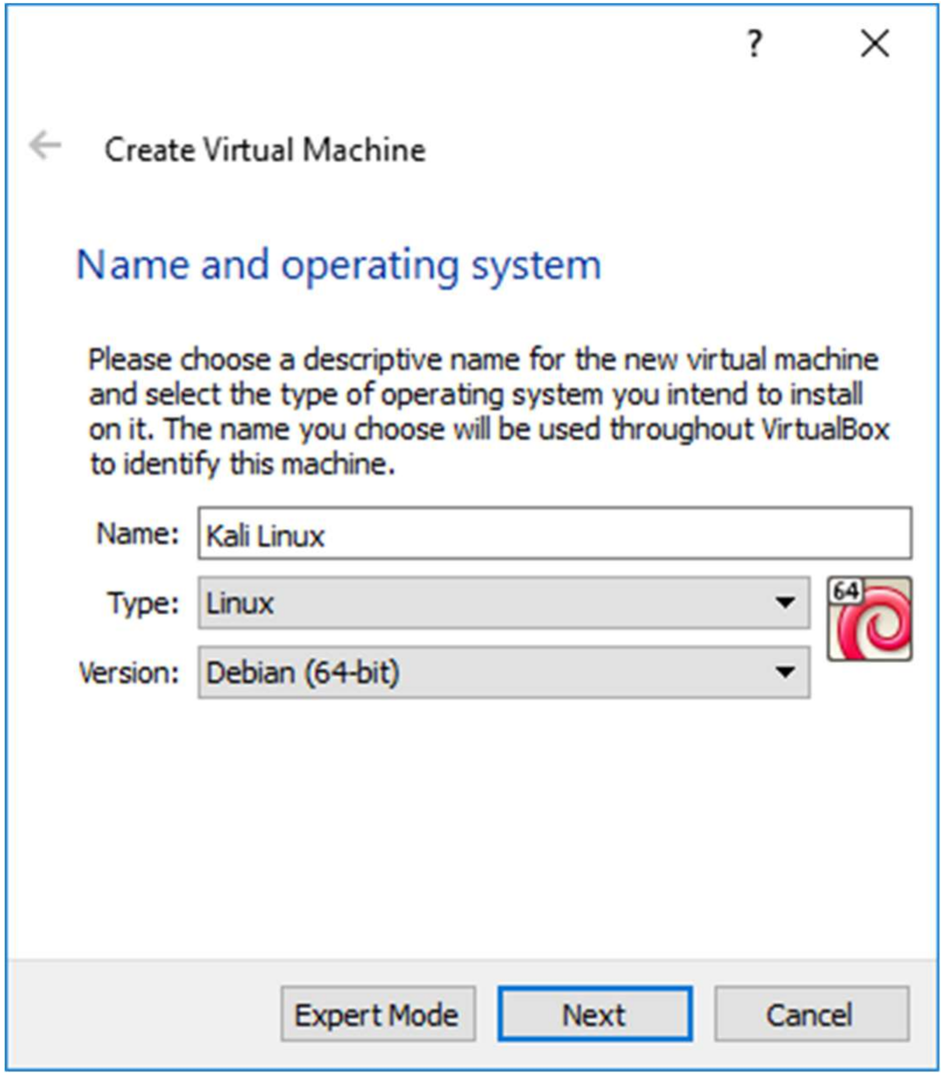
- Usage of host key:
  - Release mouse and keyboard ownership from the VM
  - Send special key combinations: host key + Del to send Ctrl+Alt+Del
  - Resizing the machine's window: e.g. to enable and leave scale mode: host key + C

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/

VirtualBox & Kali Installation



Create Virtual Machine

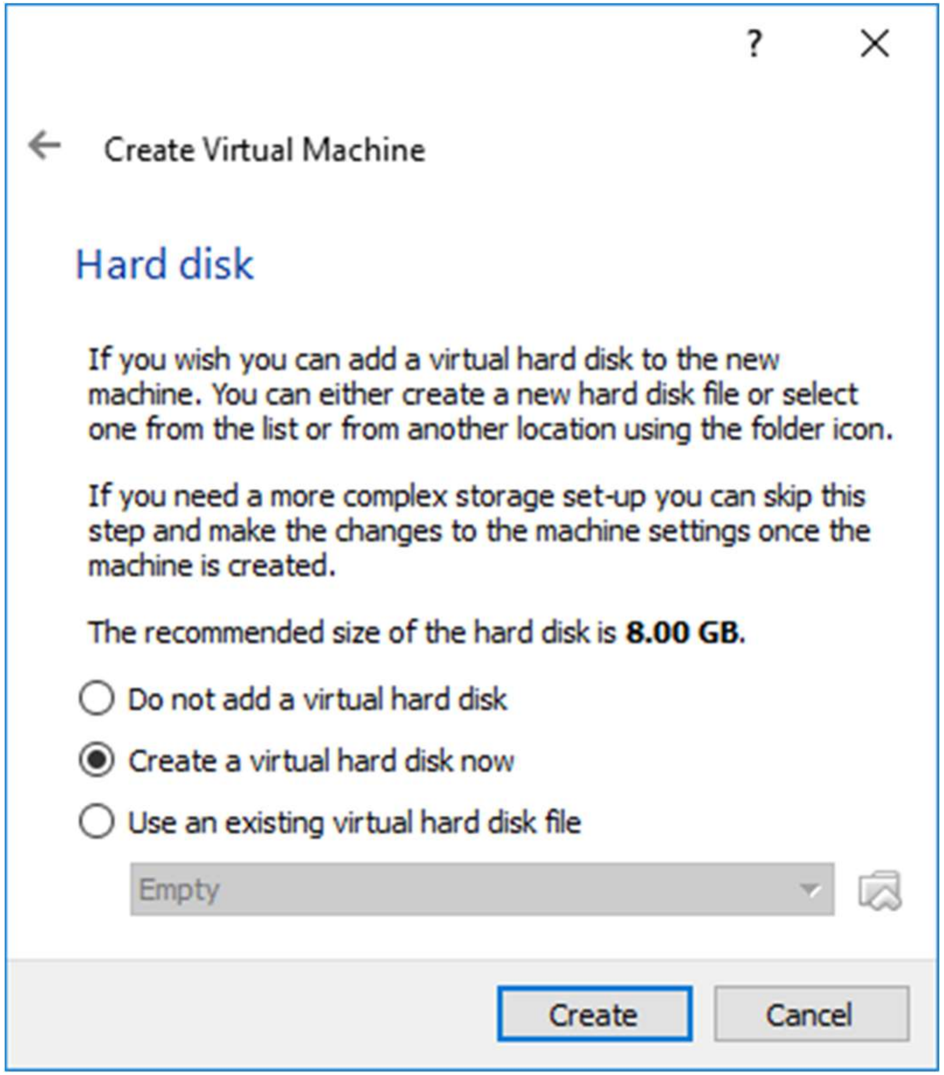
Name and operating system

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: Kali Linux

Type: Linux

Version: Debian (64-bit)



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

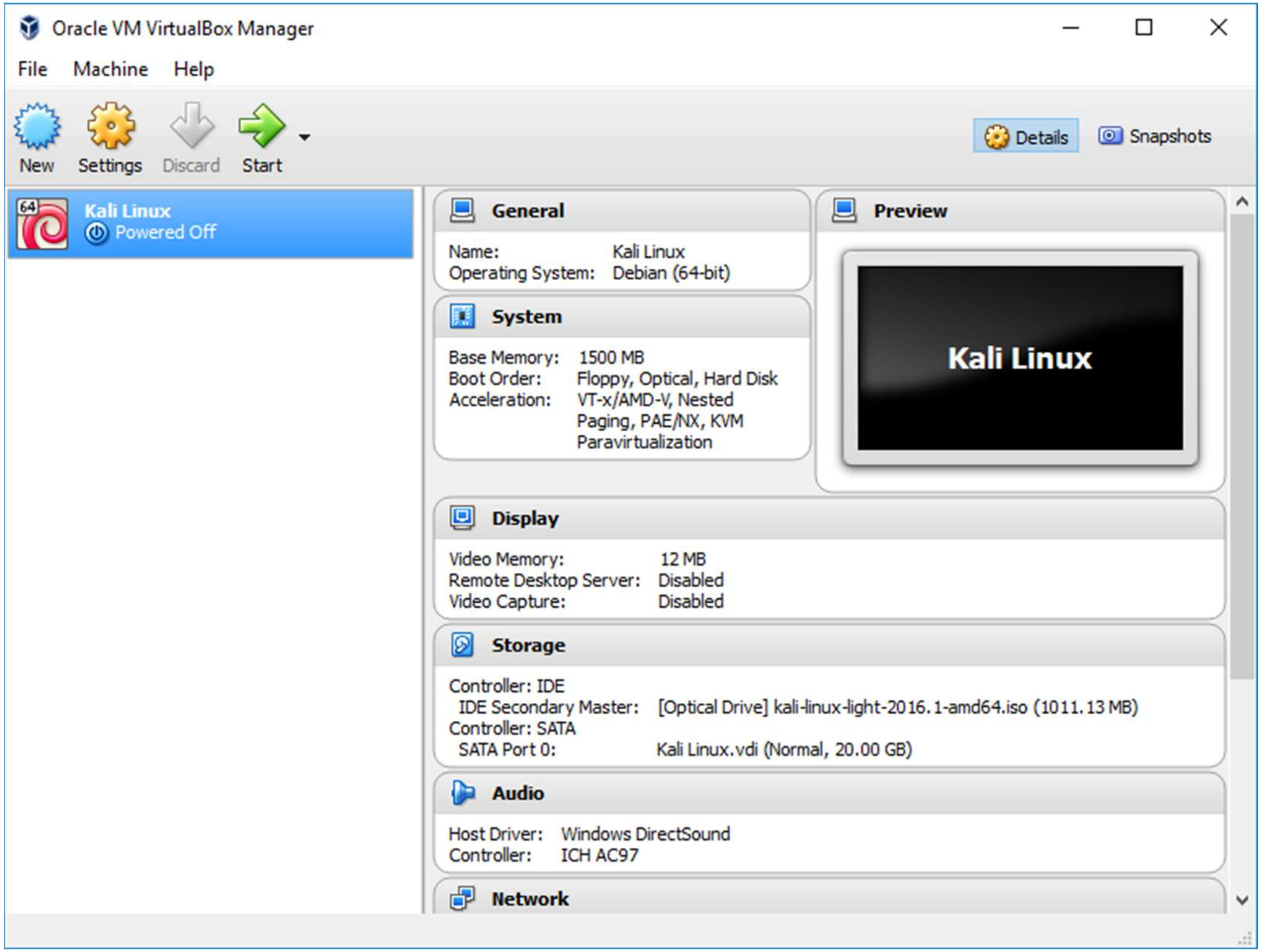
● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Empty

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

VirtualBox & Kali Installation



General

Name: Kali Linux
Operating System: Debian (64-bit)

System

Base Memory: 1500 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] kali-linux-light-2016.1-amd64.iso (1011.13 MB)
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 20.00 GB)

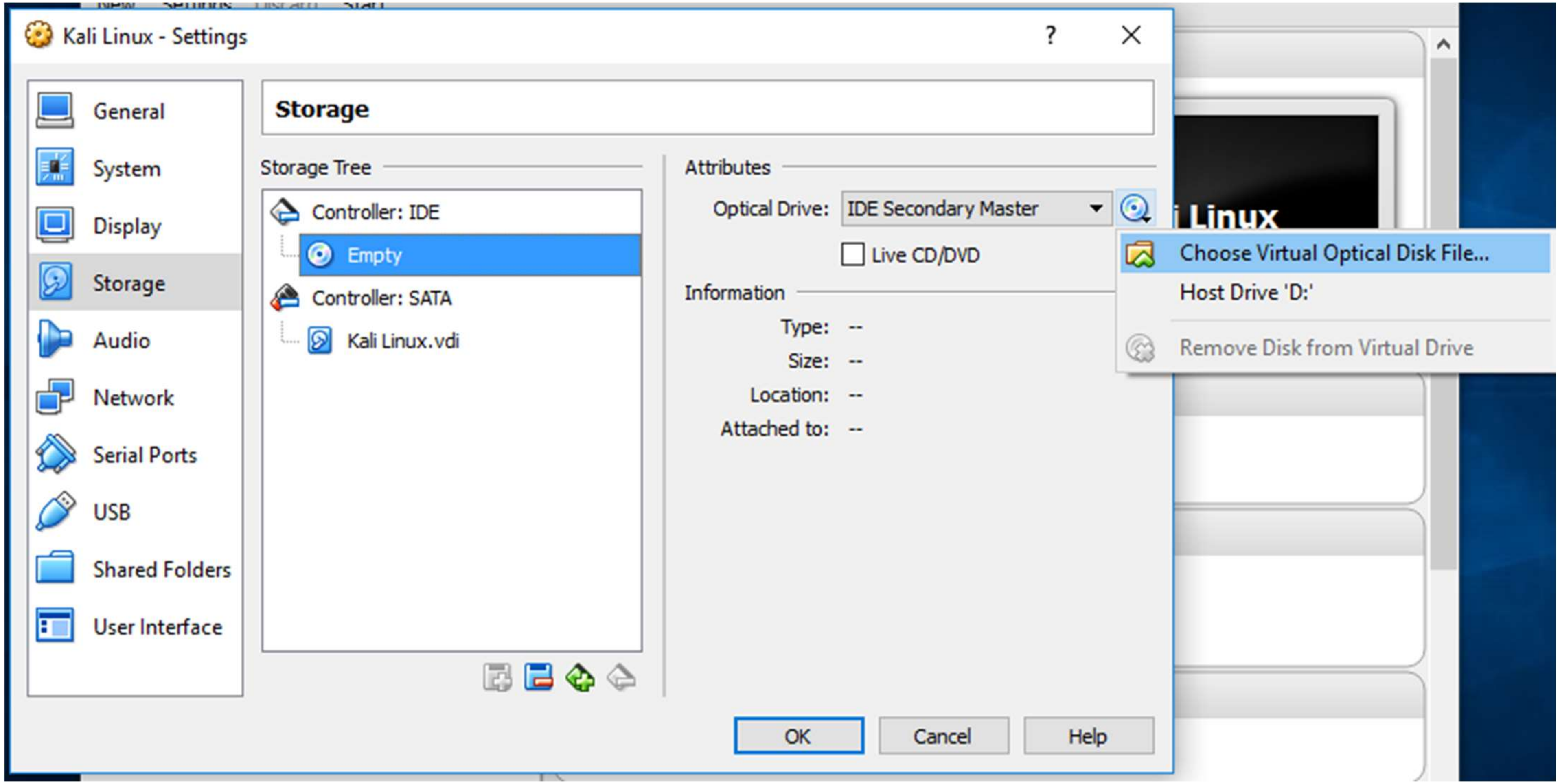
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

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

VirtualBox & Kali Installation



Kali Linux - Settings

Storage

Storage Tree

- Controller: IDE
  - Empty
- Controller: SATA
  - Kali Linux.vdi

Attributes

Optical Drive: IDE Secondary Master

□ Live CD/DVD

Information

Type: --

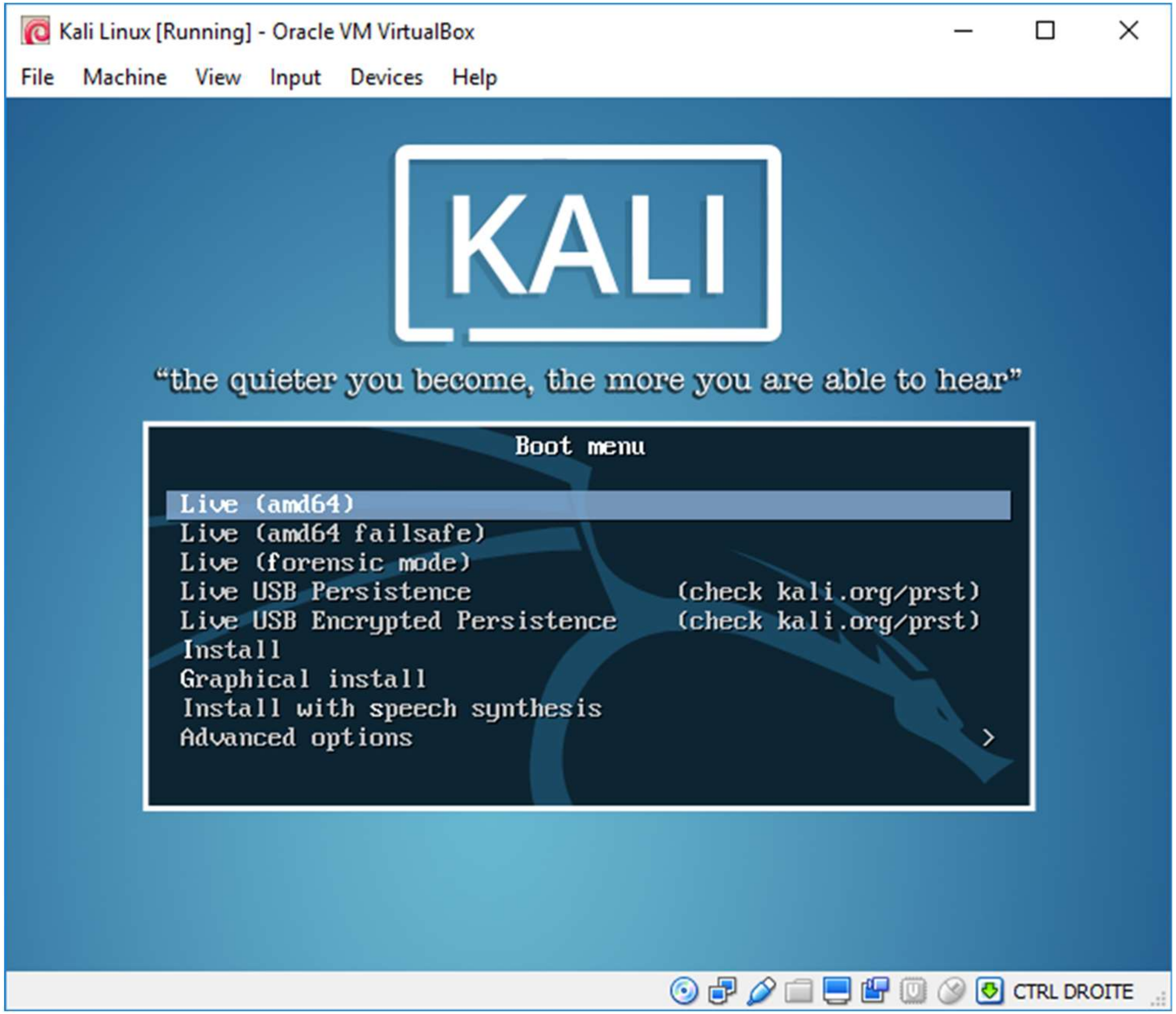
Size: --

Location: --

Attached to: --

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

Kali Linux: Boot Menu

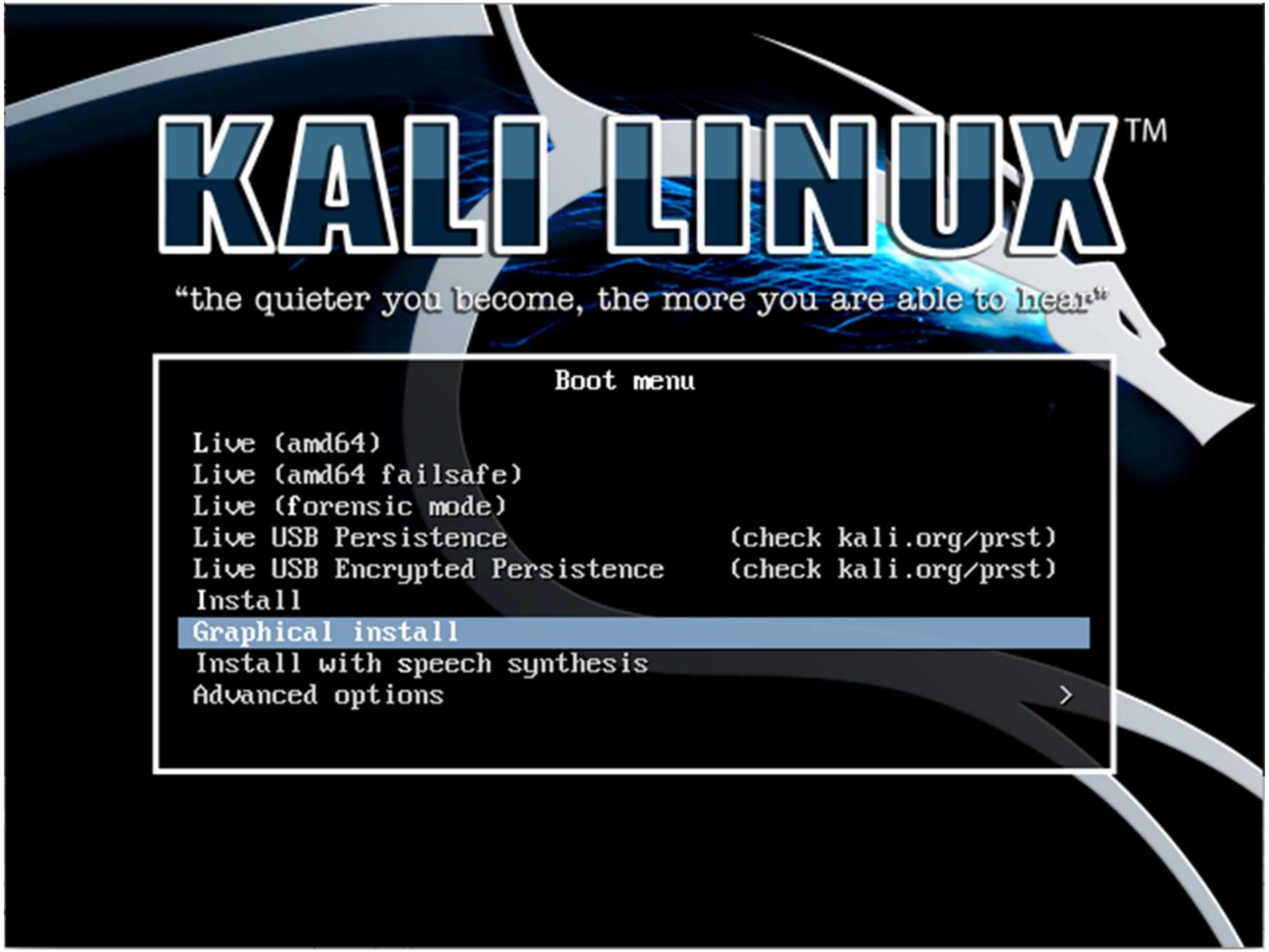


Kali Linux [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
KALI
"the quieter you become, the more you are able to hear"
CTRL DROITE

```
                    Boot menu

Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence                (check kali.org/prst)
Live USB Encrypted Persistence      (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options                                        >
```

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

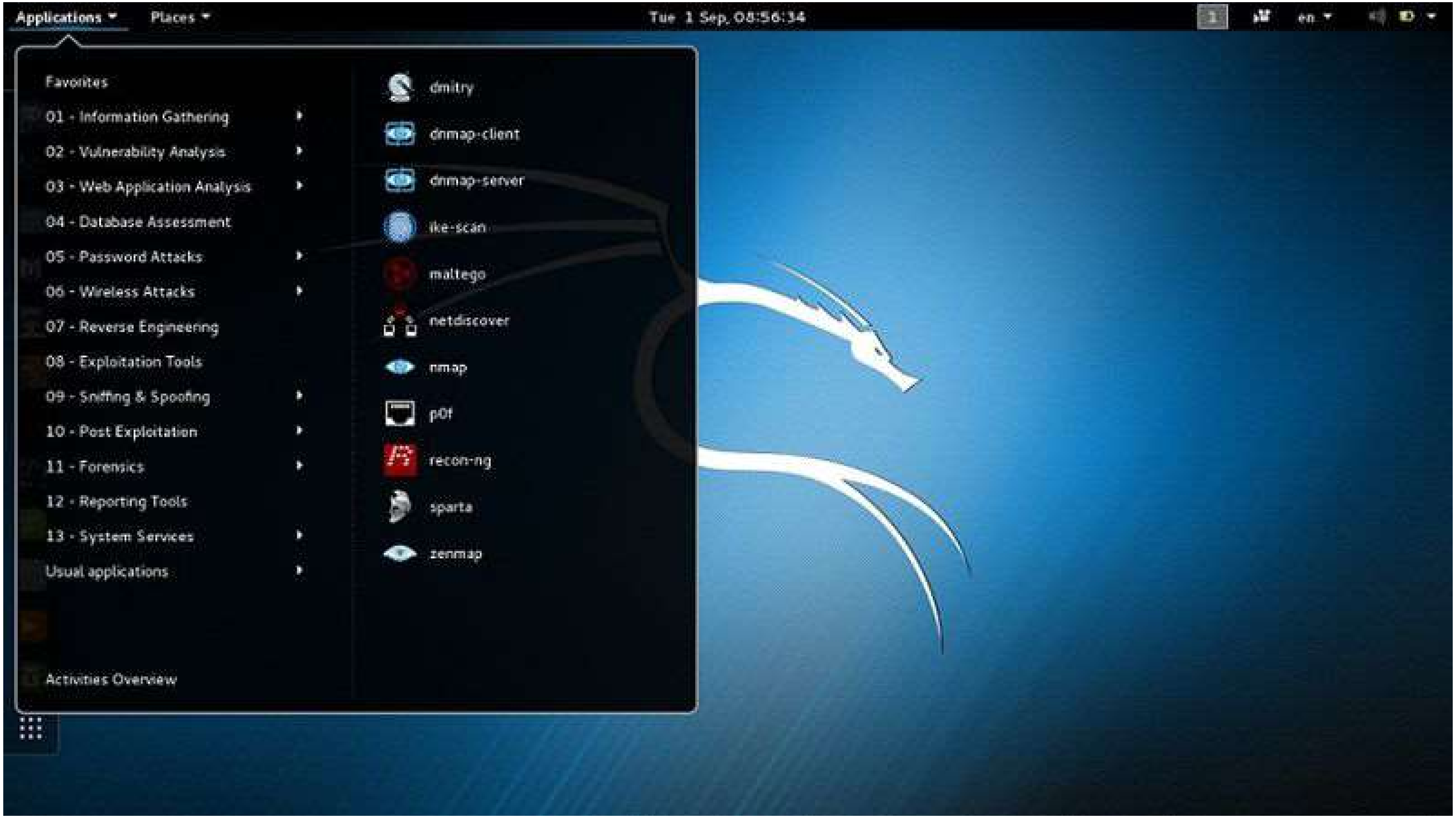
VirtualBox & Kali Installation



```
                          Boot menu

 Live (amd64)
 Live (amd64 failsafe)
 Live (forensic mode)
 Live USB Persistence                (check kali.org/prst)
 Live USB Encrypted Persistence      (check kali.org/prst)
 Install
 Graphical install
 Install with speech synthesis
 Advanced options                                          >
```

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

Kali Linux: Applications



Source: Wikipedia

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 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: 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***

Your *Lab 0* (Self-Lab)

To try in this week:

- Install VirtualBox/VMware
- Install Kali Linux
- Install Ubuntu Linux **20.04 x64**

Questions?