

MIS 5170

Operating System Security

Week 2 Hypervisors

Tonight's Plan

2

- ❑ Questions from Last Week
- ❑ Review on-line posts
- ❑ In The News
- ❑ Hypervisors
- ❑ Network Fundamentals
- ❑ Start building lab environments on desktop
- ❑ Assignment 1
- ❑ Next Week

Caution

3

- ❑ Some tools and techniques discussed and used in this course should only be used on systems you personally own, or have written permission to use.
- ❑ Some of the tools used have the potential to disrupt or break computer systems.

Wade Mackey's Advanced Penetration Testing

Questions from Last Week

4

- Questions?
 - Any follow-up questions about hypervisors from last week?
 - Type 1 - ?
 - Type 2 - ?
 - General follow-up questions?

Review On-Line Posts

5

- Top Posts
 - ▣ Post 1
 - ▣ Post 2
 - ▣ Post 3

Review On-Line Posts (cont)

6

- Questions?

In the News

7

- Dirty Cow
 - Common Vulnerabilities and Exposures site write up: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195>
 - YouTube video: <https://www.youtube.com/watch?v=kEsshExn7aE>
- NPR: Listen to the Avi Rubin recording for 11:36
<http://www.npr.org/2017/01/13/509355546/what-happens-when-hackers-hijack-our-smart-devices>
- Avi Rubin:
 - All your device can be hacked: https://embed.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?zone=npr2
 - Hacking our watches, fridges, and more: <https://www.youtube.com/watch?v=hhh3U2Swyfg>
- IOT DDoS attack
 - <http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>
 - <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

In the News

8

- ❑ Adobe, Microsoft Push Critical Security Fixes
 - ❑ <https://krebsonsecurity.com/2017/01/adobe-microsoft-push-critical-security-fixes-9/>
 - Month Without Adobe Flash Player
 - <http://krebsonsecurity.com/2015/06/a-month-without-adobe-flash-player/>
 - ❑ Thoughts?
- ❑ Extortionists Wipe Thousands of Databases, Victims Who Pay Up Get Stiffed
 - ❑ <https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/>
 - ❑ Thoughts?

In the News (cont)

9

- Questions?

Hypervisors

10

- ❑ What is a hypervisor?
- ❑ What makes up a hypervisor?
- ❑ What is the difference between a type 1 and type 2 hypervisors?
- ❑ Specific Products

Hypervisors (cont)

11

- What is a hypervisor?
 - ▣ A hypervisor or virtual machine monitor (VMM) is a piece of computer software (type 2), firmware or hardware that creates and runs virtual machines (type 1). A computer on which a hypervisor is running one or more virtual machines is defined as a host machine. Each virtual machine is called a guest machine.
 - ▣ Let look at the two different type of hypervisors:

Hypervisors (cont)

12

- Type 1
 - ESXi

```
VMware ESXi 6.5.0 (VMKernel Release Build 4564106)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Core(TM) i7-6920HQ CPU @ 2.90GHz
4 GiB Memory

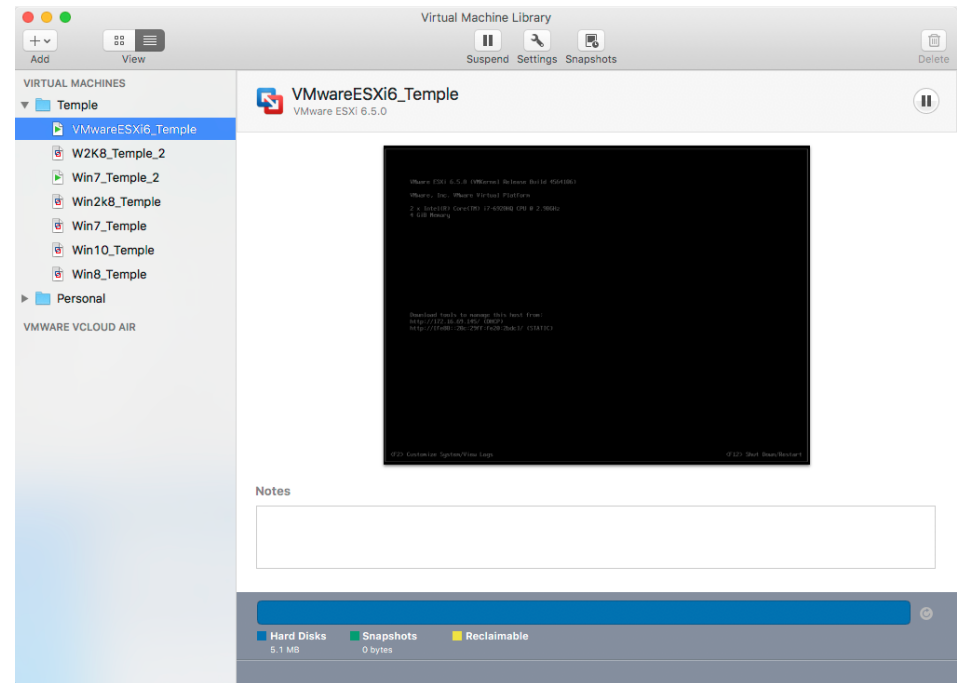
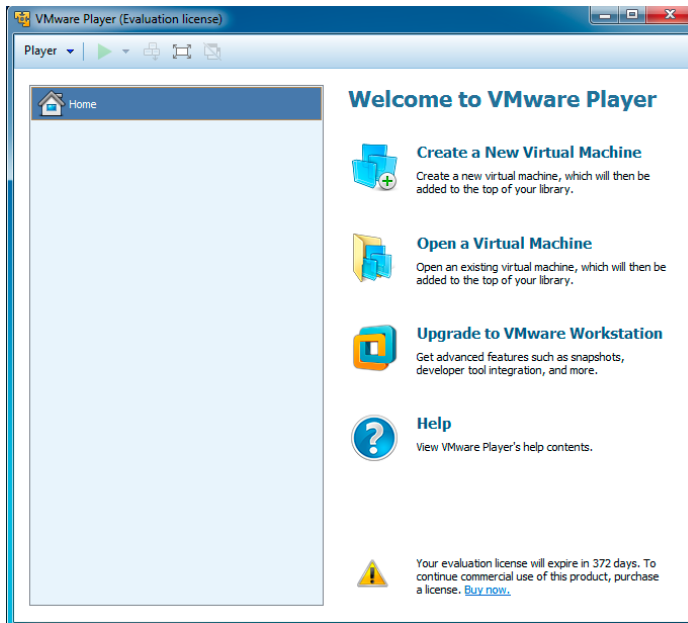
Download tools to manage this host from:
http://172.16.69.145/ (DHCP)
http://[fe80::20c:29ff:fe20:2bdc1]/ (STATIC)

<F2> Customize System/View Logs
<F12> Shut Down/Restart
```

Hypervisors (cont)

13

- Type 2
 - ▣ VMWare Player
 - ▣ VMWare Fusion



Hypervisors (cont)

14

- What makes up a hypervisor?
 - ▣ As we saw last week, but as a refresher:
 - ▣ Hypervisor are made up of the following
 - Hardware – a computer and/or server
 - OS – not part of a type 1 hypervisor
 - VMM/Hypervisor – Virtual Machine Manager is another name for a hypervisor. This is an application or OS creating a virtual BIOS and hardware layer to the Guest OS running on top of or next to other applications
 - Guest OS – an OS running in a virtual container/environment. The guest OS mostly behaves as if it were the only OS running on the underlying hardware.

Hypervisors (cont)

15

- What is the difference between a type 1 and type 2 hypervisor?
 - ▣ Type 1 hypervisor
 - A type 1 hypervisor is running directly on the hardware with no OS between it and the hardware it is scheduling for the Guest OS's
 - ▣ Type 2 hypervisor
 - A type 2 hypervisor is an application running on top of an OS, needing to honor all requirements of the OS it is installed. Otherwise it is very similar to a type 1 hypervisor, but resources are shared equally for applications that the user might be running next to the hypervisor.?

Hypervisors (cont)

16

- ❑ Specific Products
 - ❑ VMWare
 - Type 1
 - ESXi (<http://www.vmware.com/products/vsphere-hypervisor.html>)
 - Type 2
 - Player
 - Fusion
 - Workstation
 - ❑ Hyper-V
 - Can be both Type 1 or Type 2; based on the installation options you choose (<https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2012?i=1>)
 - ❑ Oracle
 - <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>

Hypervisors (cont)

17

- Questions?

Start Building Lab Environment

18

- ❑ Download all software
- ❑ Review requirements
- ❑ Review installation
- ❑ Learn VM Software

Start Building Lab Environment (cont)

19

- ❑ Download all software
 - ❑ Download Site:
<https://e5.onthehub.com/WebStore/OfferingDetails.aspx?o=4dc77b3d-cc51-e111-8056-f04da23e67f6&pmv=a4fc11a0-0a57-e011-bd14-0030487d8897&ws=933e35a0-db9b-e011-969d-0030487d8897&vsro=8>
 - ❑ VMware Workstation 12 for Windows
 - ❑ Windows 7 Professional with Service Pack 1 32/64-bit (English) - Microsoft Imagine
 - ❑ Windows Server 2008 R2 Enterprise with SP1 64-bit (English) - Microsoft Imagine

Start Building Lab Environment (cont)

20

❑ VMware Workstation 12 for Windows

VMware Workstation 12 ▲



VMware Workstation 12 Pro continues VMware's tradition of delivering leading edge features and performance that technical professionals rely on every day when working with virtual machines. With support for the latest version of Windows and Linux, the latest processors and hardware, and the ability to connect to VMware vSphere and vCloud Air, it's the perfect tool to increase productivity, save time and conquer the cloud.

Choose a platform:

Windows

VMware Workstation 12 for Windows


Available to: Faculty/Staff

Workstation requires a 64-bit processor and 64-bit host operating system.

You will be able to place an order for this product again in 12 months after the initial order.

The license you will receive with this offering is valid 12 months starting with the 1st of the month the offering was ordered.

Free

 Add to Cart

Start Building Lab Environment (cont)

21

- ❑ Windows 7 Professional with Service Pack 1 32/64-bit (English) - Microsoft Imagine

Windows 7 Professional ▲




Simplify everyday tasks: find something instantly, compare documents side-by-side, or easily back-up your complete system over a network. Enjoy a PC that works the way you want it to; supports 64-bit technologies and offers XP Mode for your business productivity applications. Make new things possible: watch Internet TV, pause, rewind, and record TV or use Touch to interact with your PC in new ways.

Windows 7 Professional with Service Pack 1 32/64-bit (English) - Microsoft Imagine

Available to: Students/Faculty/Staff

Free

 Add to Cart

Backup media: Available in most countries



Start Building Lab Environment (cont)

22

- ❑ Windows Server 2008 R2 Enterprise with SP1 64-bit (English) - Microsoft Imagine

Windows Server 2008 R2 Standard-Enterprise-Datacenter-Web ▲



Windows Server 2008 R2 builds on the award-winning foundation of Windows Server 2008, expanding existing technology and adding new features to enable IT professionals to increase the reliability and flexibility of their server infrastructures.

Choose a language:

English

Windows Server 2008 R2 Datacenter with SP1 64-bit (English) - Microsoft Imagine

Available to: Students/Faculty/Staff

Free

Add to Cart

Windows Server 2008 R2 Enterprise with SP1 64-bit (English) - Microsoft Imagine

Available to: Students/Faculty/Staff

Free

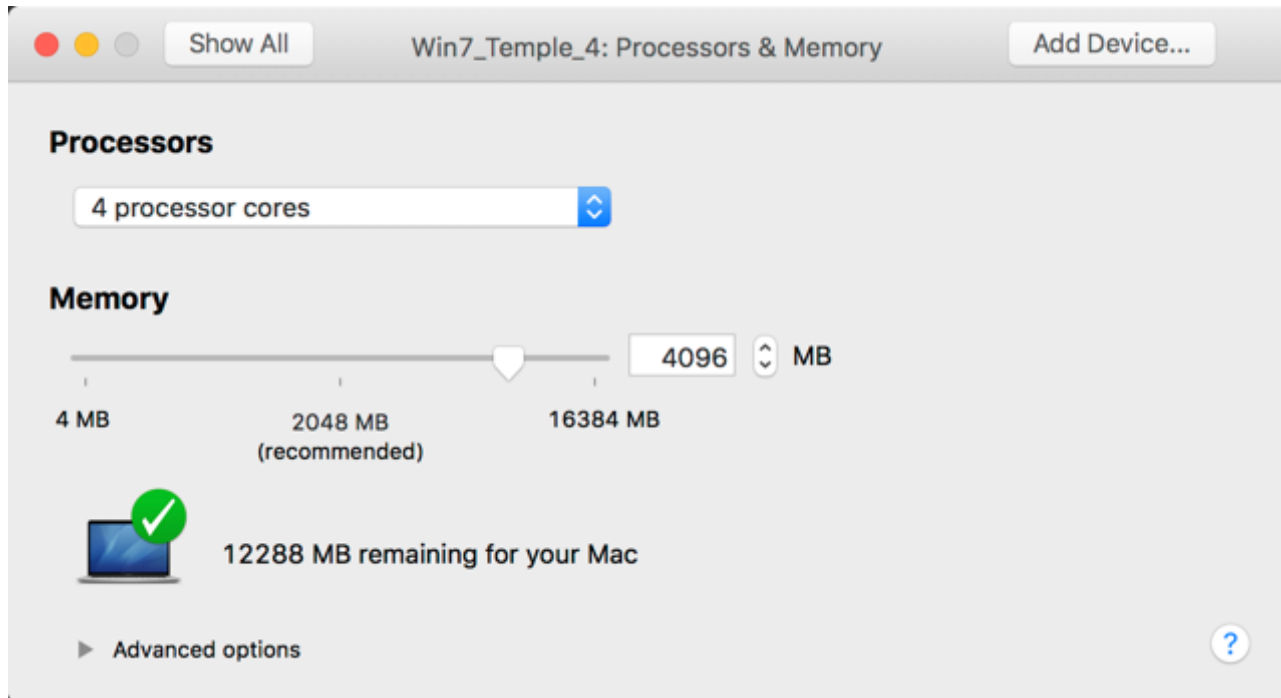
Add to Cart



Start Building Lab Environment (cont)

23

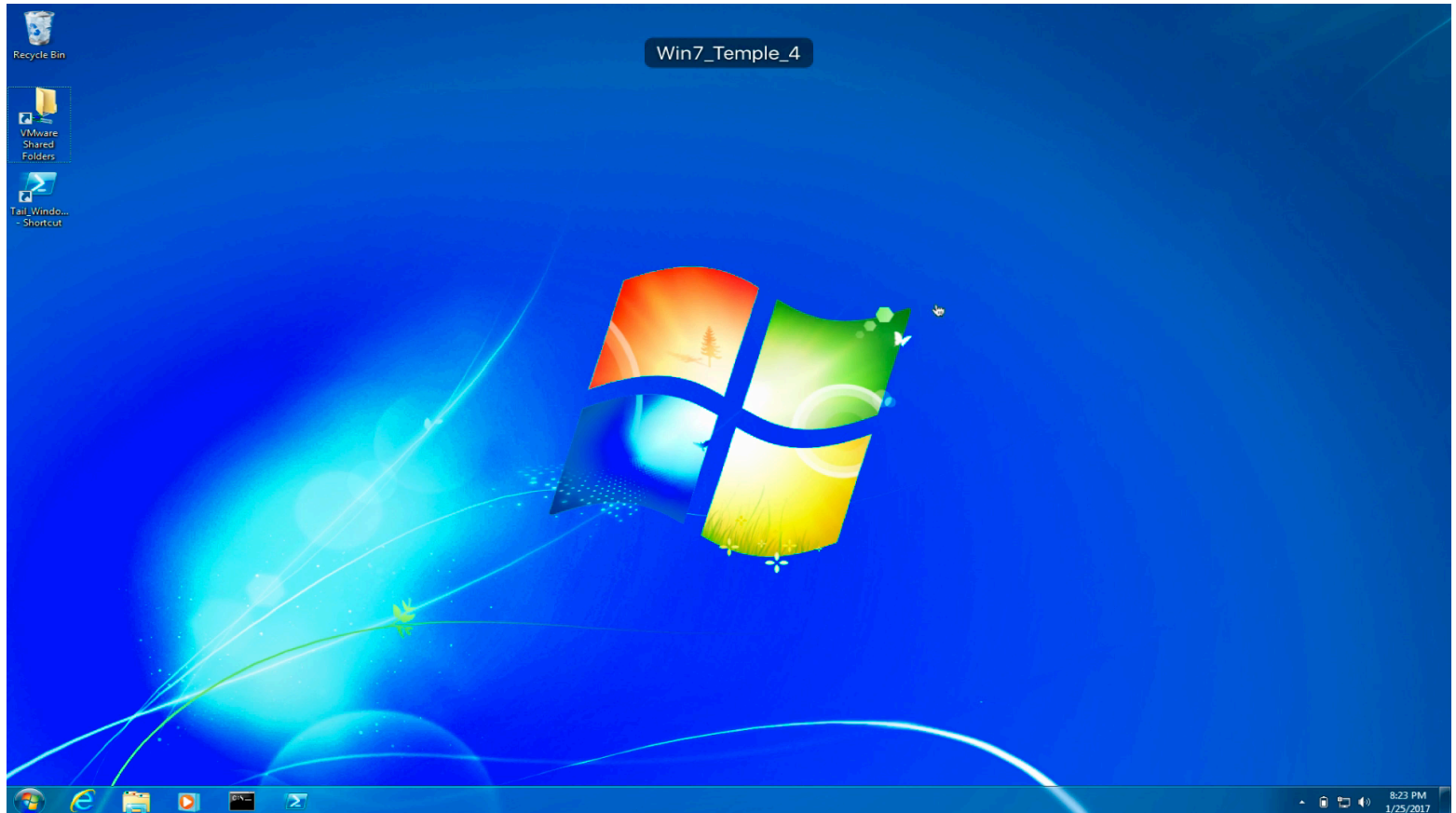
- ❑ Review requirements



Start Building Lab Environment (cont)

24

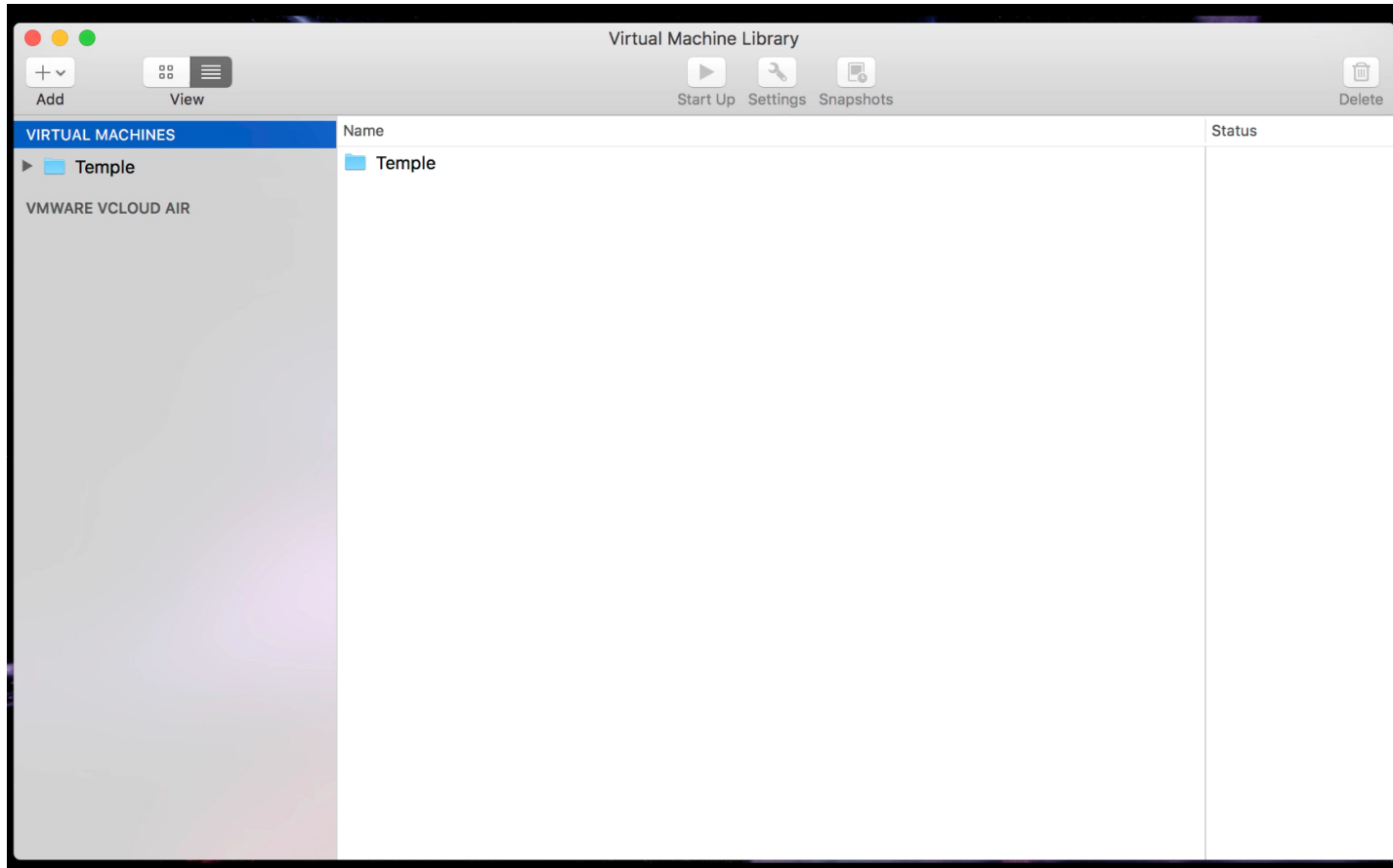
□ Hypervisor installation



Start Building Lab Environment (cont)

25

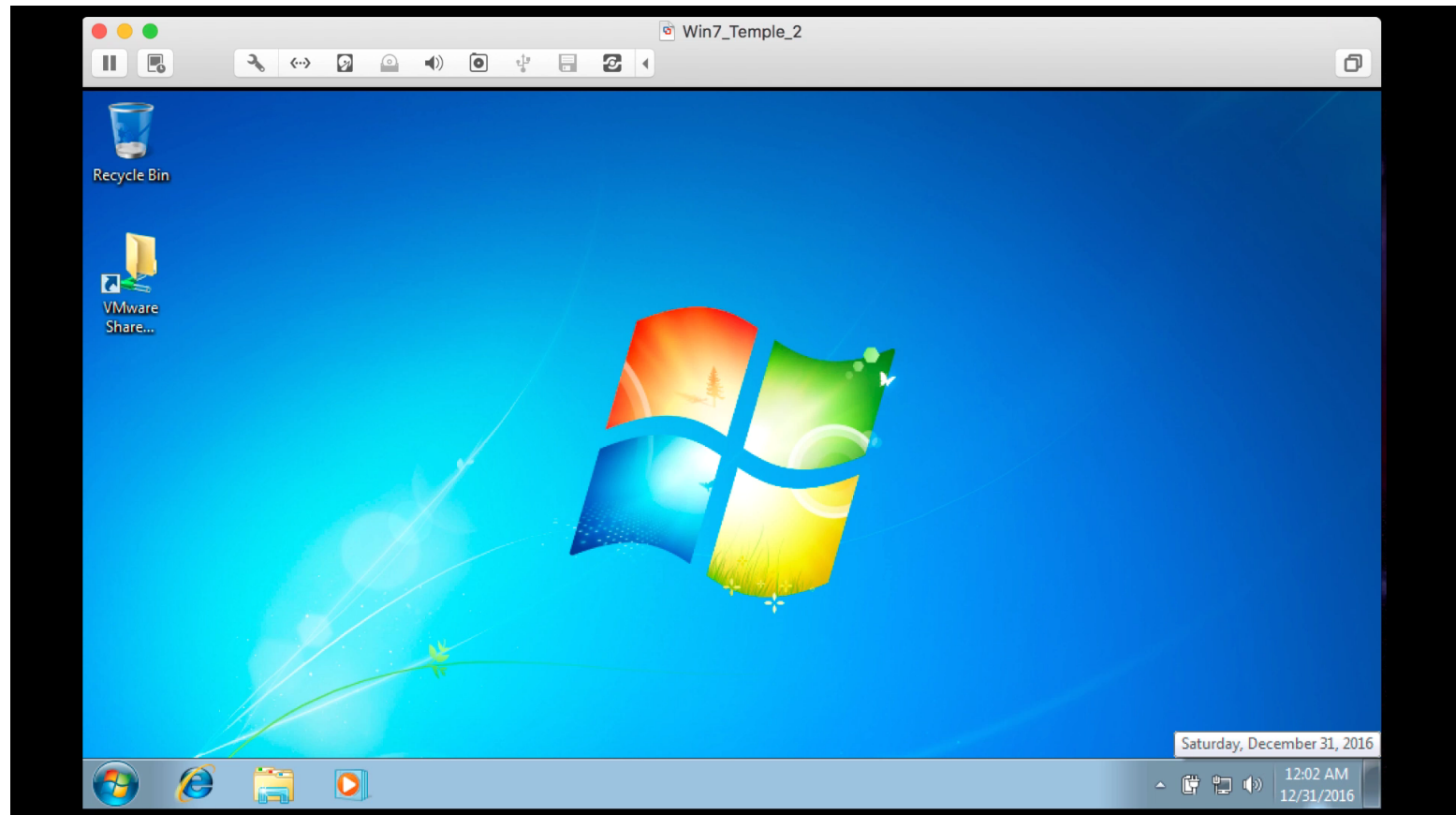
❑ Install Windows 7



Start Building Lab Environment (cont)

26

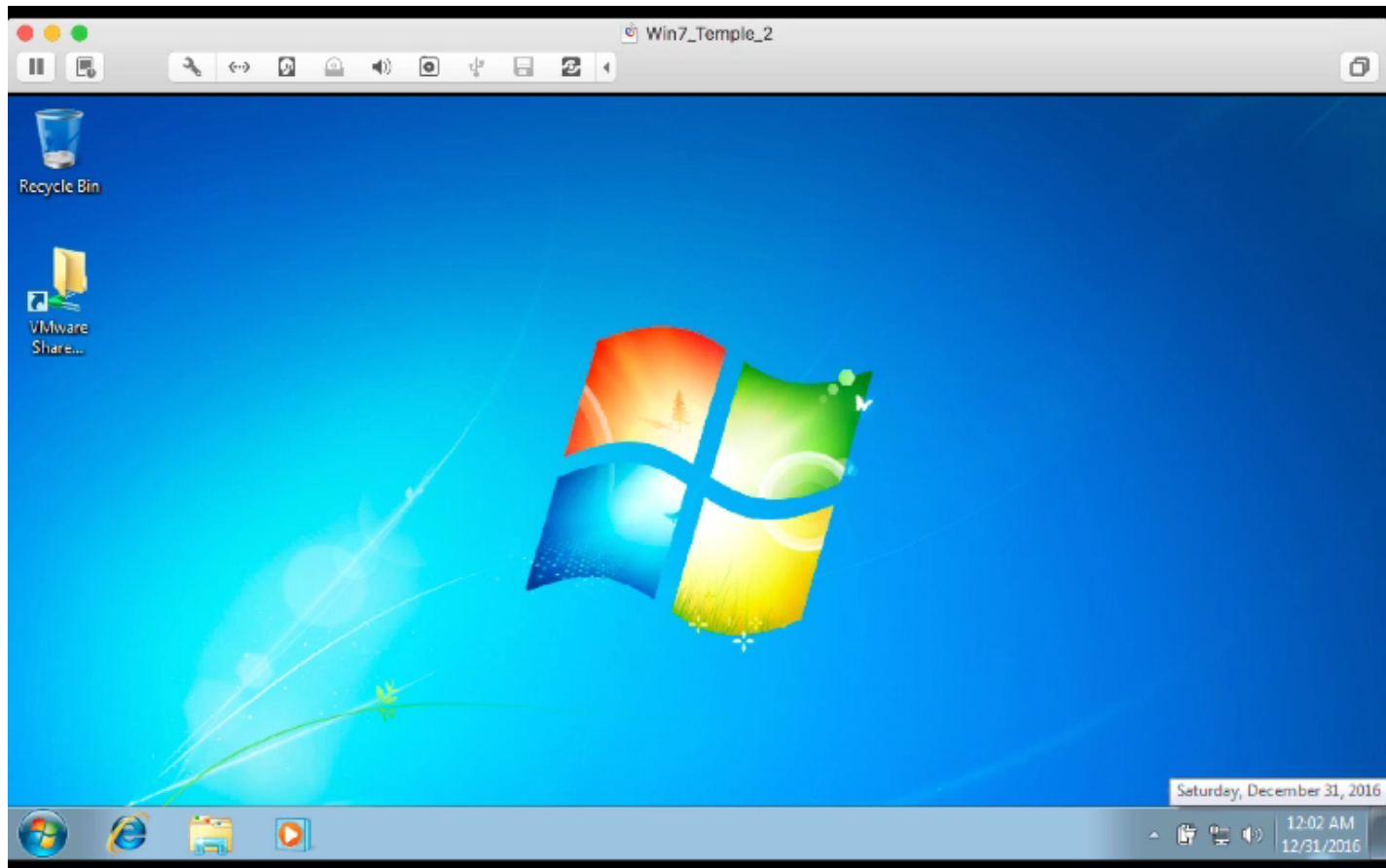
□ Install Cygwin



Start Building Lab Environment (cont)

27

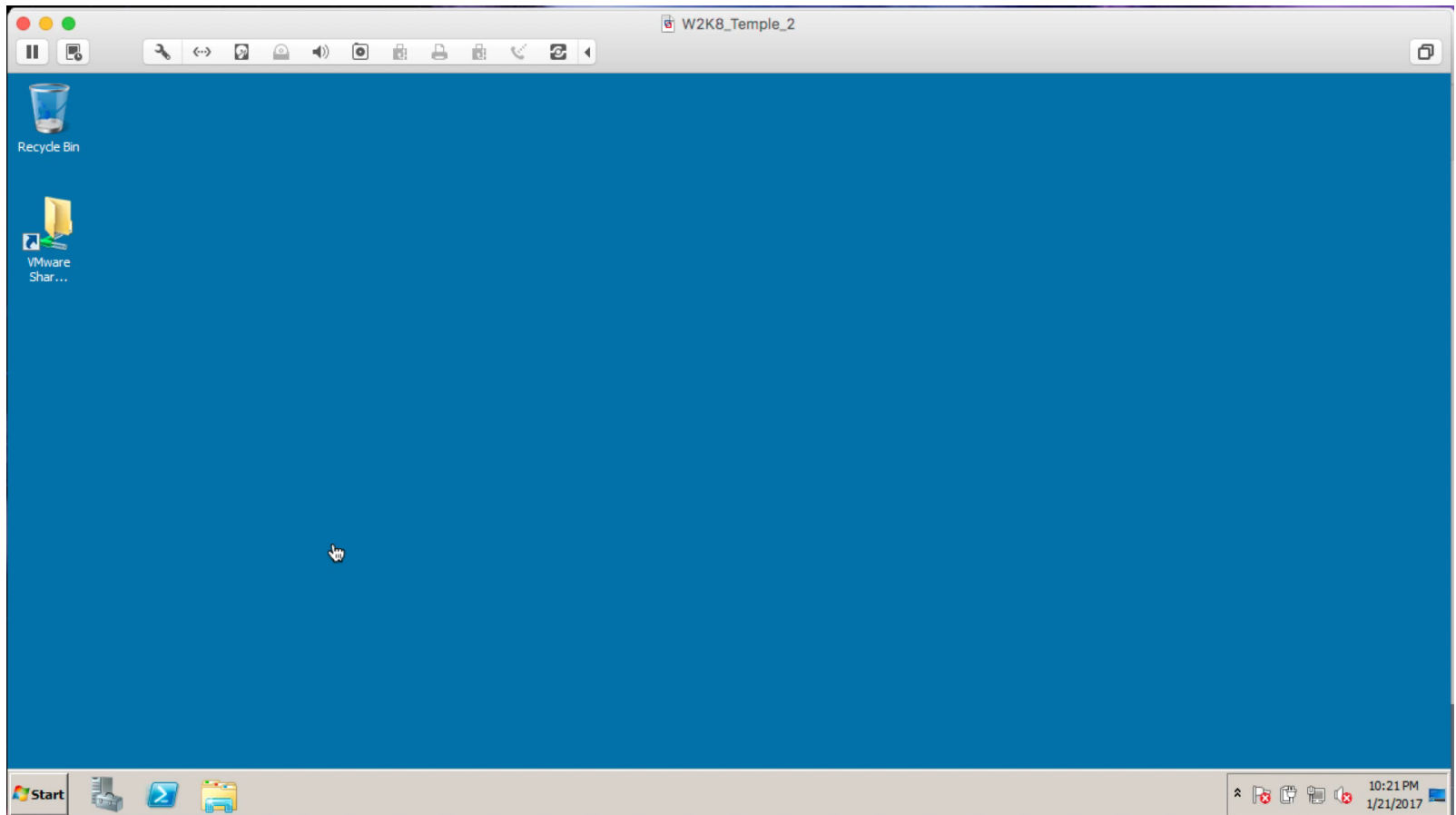
- Install Patches for Windows 7



Start Building Lab Environment (cont)

28

- Setup PowerShell to Watch Windows Update



Start Building Lab Environment (cont)

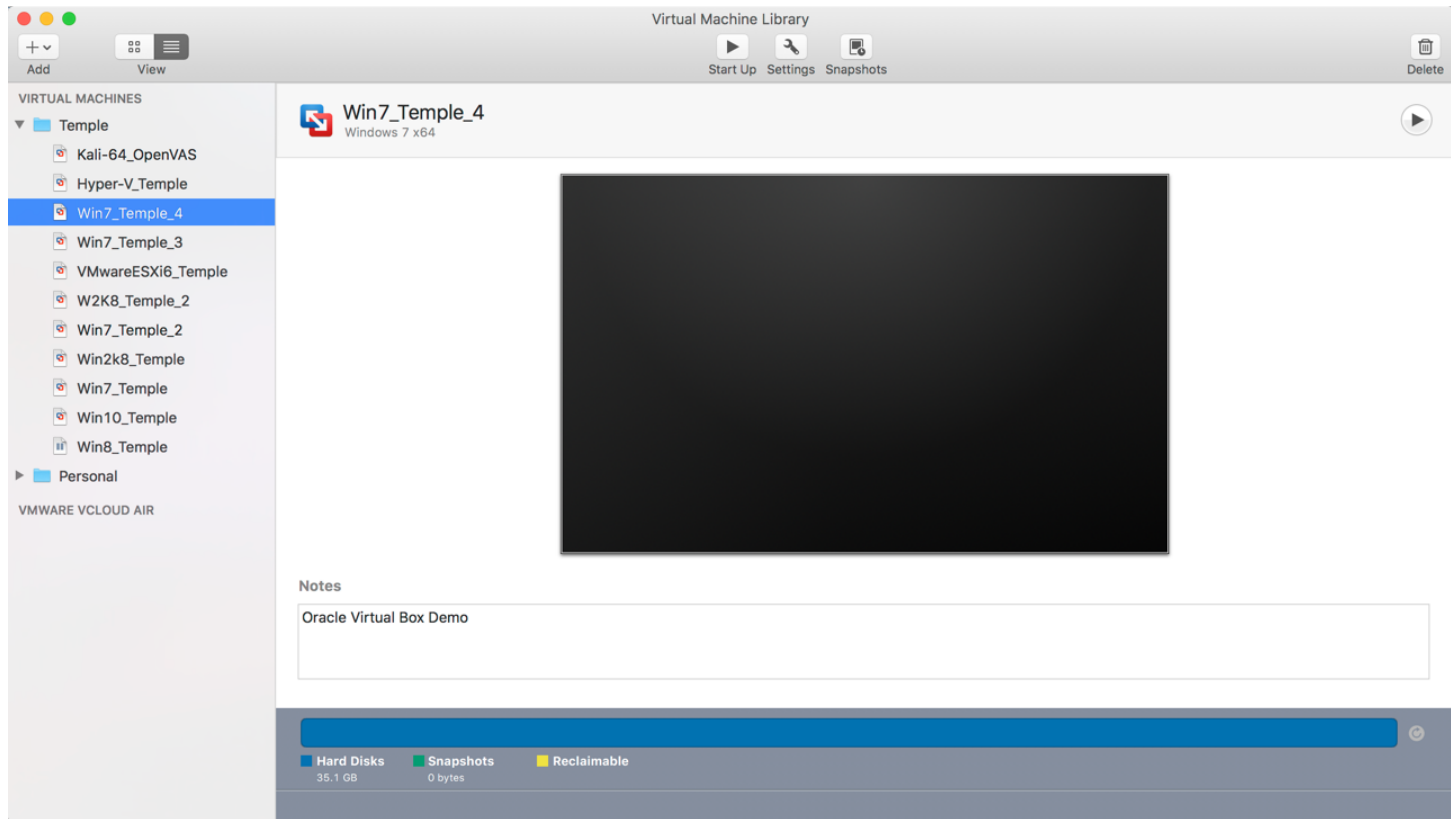
29

- Virtual Machines
 - Window 7 (1-4)
 - Windows 2008 R2 Enterprise (1 Domain Controller)
 - Kali – (2 = 1 – testing, 1 - OpenVAS scanner)

Start Building Lab Environment (cont)

30

□ Review installation



Start Building Lab Environment (cont)

31

- Learn VM Software
 - ▣ Start Demo

Start Building Lab Environment (cont)

32

- Questions?

Network Fundamentals

33

- IP v4
 - Cidr Notation
 - Route Statements
 - IPSec
 - TCP/IP and Network Architecture and its impact on Operating System Security

Network Fundamentals (cont)

34

□ CIDR Notation

CIDR Notation	Total number of Addresses	Network Mask	Description	CIDR Notation	Total number of Addresses	Network Mask	Description
/0	4,294,967,296	0.0.0.0	Every Address				
/1	2,147,483,648	128.0.0.0	128 /8 nets	/17	32,768	255.255.128.0	128 / 24 nets
/2	1,073,741,824	192.0.0.0	64 /8 nets	/18	16,384	255.255.192.0	64 / 24 nets
/3	536,870,912	224.0.0.0	32 /8 nets	/19	8,192	255.255.224.0	32 / 24 nets
/4	268,435,456	240.0.0.0	16 /8 nets	/20	4,096	255.255.240.0	16 / 24 nets
/5	134,217,728	248.0.0.0	8 /8 nets	/21	2,048	255.255.248.0	8 / 24 nets
/6	67,108,864	252.0.0.0	4 /8 nets	/22	1,024	255.255.252.0	4 / 24 nets
/7	33,554,432	254.0.0.0	2 /8 nets	/23	512	255.255.254.0	2 / 24 nets
/8	16,777,214	255.0.0.0	1 /8 net	/24	256	255.255.255.0	1 / 24 nets
/9	8,388,608	255.128.0.0	128 / 16 nets	/25	128	255.255.255.128	Half of a /24
/10	4,194,304	255.192.0.0	64 / 16 nets	/26	64	255.255.255.192	Fourth of a /24
/11	2,097,152	255.224.0.0	32 / 16 nets	/27	32	255.255.255.224	1/8 th of a /24
/12	1,048,576	255.240.0.0	16 / 16 nets	/28	16	255.255.255.240	1/16 th of a /24
/13	524,288	255.248.0.0	8 / 16 nets	/29	8	255.255.255.248	5 usable addresses
/14	262,144	255.252.0.0	4 / 16 nets	/30	4	255.255.255.252	1 usable address
/15	131,072	255.254.0.0	2 / 16 nets	/31	2	255.255.255.254	Unusable
/16	65,536	255.255.0.0	1 / 16 nets	/32	1	255.255.255.255	Single Host

Network Fundamentals (cont)

35

□ Route Statements (route print)

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
169.254.0.0                255.255.0.0      On-link         169.254.6.11     266
169.254.6.11              255.255.255.255 On-link         169.254.6.11     266
169.254.255.255           255.255.255.255 On-link         169.254.6.11     266
192.168.25.0               255.255.255.0    On-link         192.168.25.1     276
192.168.25.1              255.255.255.255 On-link         192.168.25.1     276
192.168.25.255            255.255.255.255 On-link         192.168.25.1     276
192.168.56.0               255.255.255.0    On-link         192.168.56.1     266
192.168.56.1              255.255.255.255 On-link         192.168.56.1     266
192.168.56.255            255.255.255.255 On-link         192.168.56.1     266
192.168.233.0              255.255.255.0    On-link         192.168.233.1    276
192.168.233.1              255.255.255.255 On-link         192.168.233.1    276
192.168.233.255           255.255.255.255 On-link         192.168.233.1    276
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         169.254.6.11     266
224.0.0.0                  240.0.0.0        On-link         192.168.56.1     266
224.0.0.0                  240.0.0.0        On-link         192.168.25.1     276
224.0.0.0                  240.0.0.0        On-link         192.168.233.1    276
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         169.254.6.11     266
255.255.255.255           255.255.255.255 On-link         192.168.56.1     266
255.255.255.255           255.255.255.255 On-link         192.168.25.1     276
255.255.255.255           255.255.255.255 On-link         192.168.233.1    276
=====
```

Network Fundamentals (cont)

36

- ❑ Routing Table Help: <https://technet.microsoft.com/en-us/library/dd379495%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396>

Network Fundamentals (cont)

37

- IPsec
 - ▣ IPsec (Internet Protocol Security) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
 - ▣ <https://en.wikipedia.org/wiki/IPsec> (Reference)
 - AH – Authentication Headers
 - ESP – Encapsulating Security Payloads

Network Fundamentals (cont)

38

- Questions?

Next Week

39

- ❑ Questions from Last Week
- ❑ Scripting
 - ❑ PowerShell
 - ❑ Python
 - ❑ Appropriate permissions
 - Access Control
 - ❑ Limit services
 - ❑ Shares
 - Windows file shares / ACLs
 - ❑ Questions about Assignment 1 (Due Feb 8)

Assignment 1 Overview

40

- ❑ Requirements – a helpdesk style document and how-to video
 - ❑ Build a video of what you did; overview is fine
 - ❑ 1 – 2 pages on the main steps and sub-steps;
 - ❑ Create a patched Windows 7 Pro 64-bit OS using a type 2 hypervisor.
 - ❑ Create a Snap-Shot of patched windows 7 box for testing of installing software and show how to install and revert back to before software being installed. Note software is not important, but learning the interface of you hypervisor is what you want to show.
- ❑ Due Date: Feb 8th