

MIS 5170

## Operating System Security

# Week 10

## Unix/Linux basics

# Tonight's Plan

2

- Download Kali
- Install Kali
- Questions from Last Week
- Review on-line posts
- In The News
- Unix/Linux Basics
- Scripting
- Appropriate Permissions
- Assignment 3 Last Minute Questions
- Assignment 4 Overview
- Next Week
- Quiz

# Install Kali

3

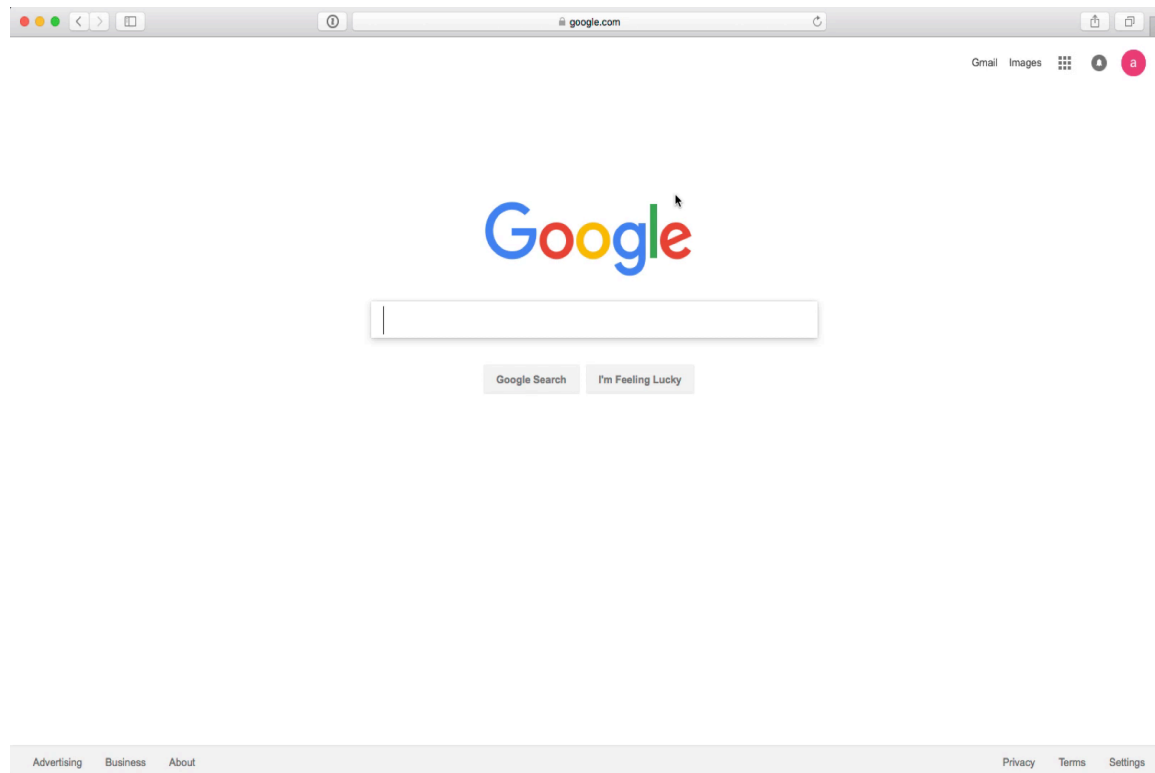
- ❑ Download Kali
- ❑ Setup VM for Kali
- ❑ Install Kali
- ❑ Next Steps

# Download Kali

4

## ❑ Download Kali

❑ <https://www.kali.org/downloads/>



# Verify Download

5

- ❑ Verify Download of Kali
  - ❑ Calculate the sha256sum from download.
  - ❑ MAC
    - `shasum -a 256 kali-linux-2016.2-amd64.iso`
  - ❑ PowerShell
    - `$Alg = [security.cryptography.hashalgorithm]::create("SHA256")`
    - `$File = [io.file]::readallbytes("<File Name")`
    - `$bytes = $Alg.ComputeHash($File)`
    - `-join ($bytes | foreach {"{0:x2}" -f $_})`

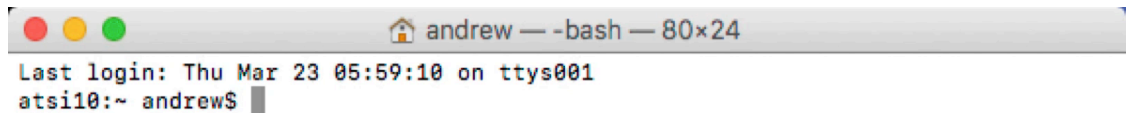
Image Name	Download	Size	Version	sha256sum
Kali 64 bit	<a href="#">ISO</a>   <a href="#">Torrent</a>	2.9G	2016.2	1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431

# Verify Download

6

## □ Verify Download of Kali

- 1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431

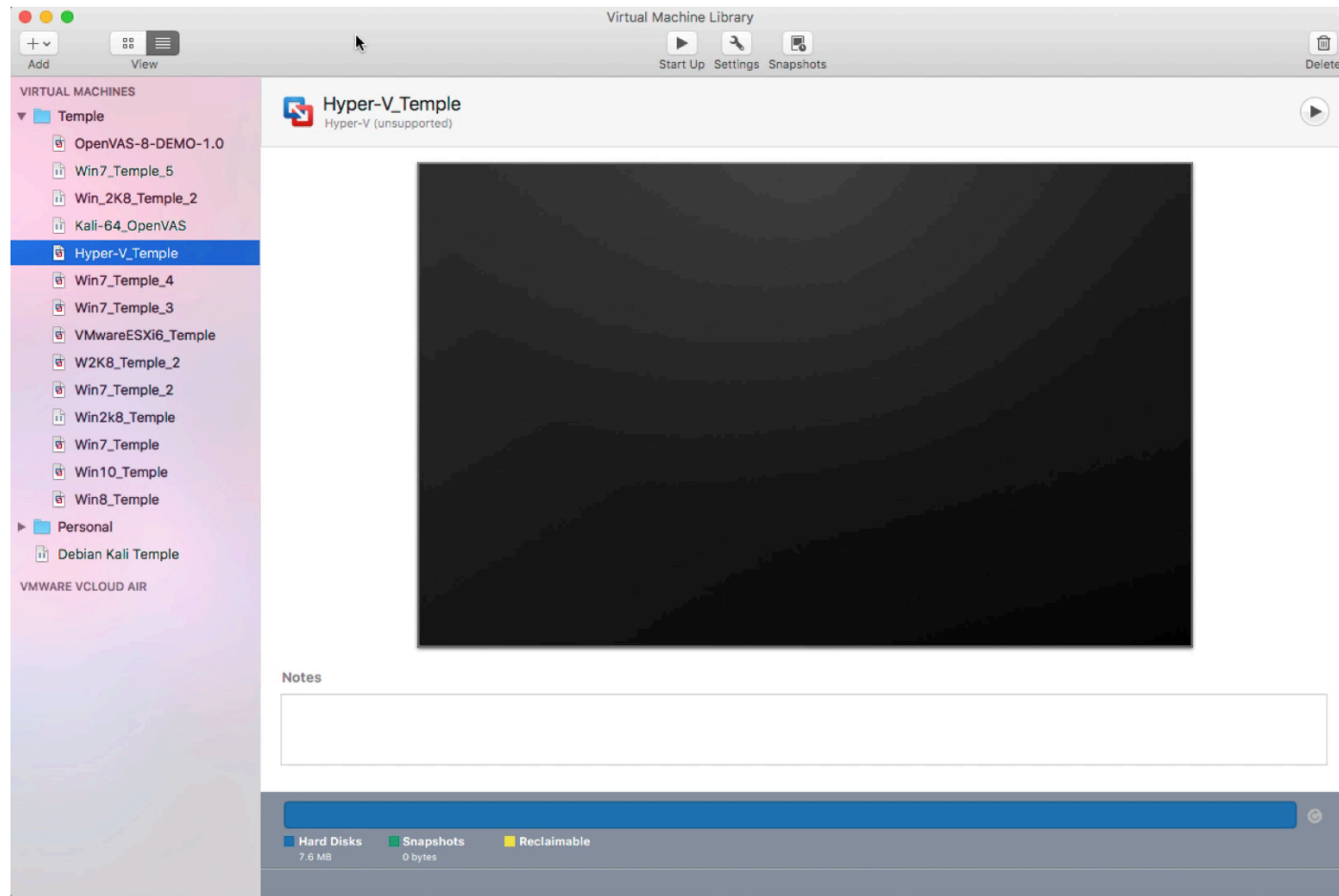
A screenshot of a terminal window. The title bar shows a home icon, the name 'andrew', and the command '-bash' with a window size of '80x24'. The terminal content shows the last login time as 'Thu Mar 23 05:59:10 on ttys001' and the current prompt as 'atsi10:~ andrew\$' with a cursor.

```
andrew — -bash — 80x24
Last login: Thu Mar 23 05:59:10 on ttys001
atsi10:~ andrew$
```

I

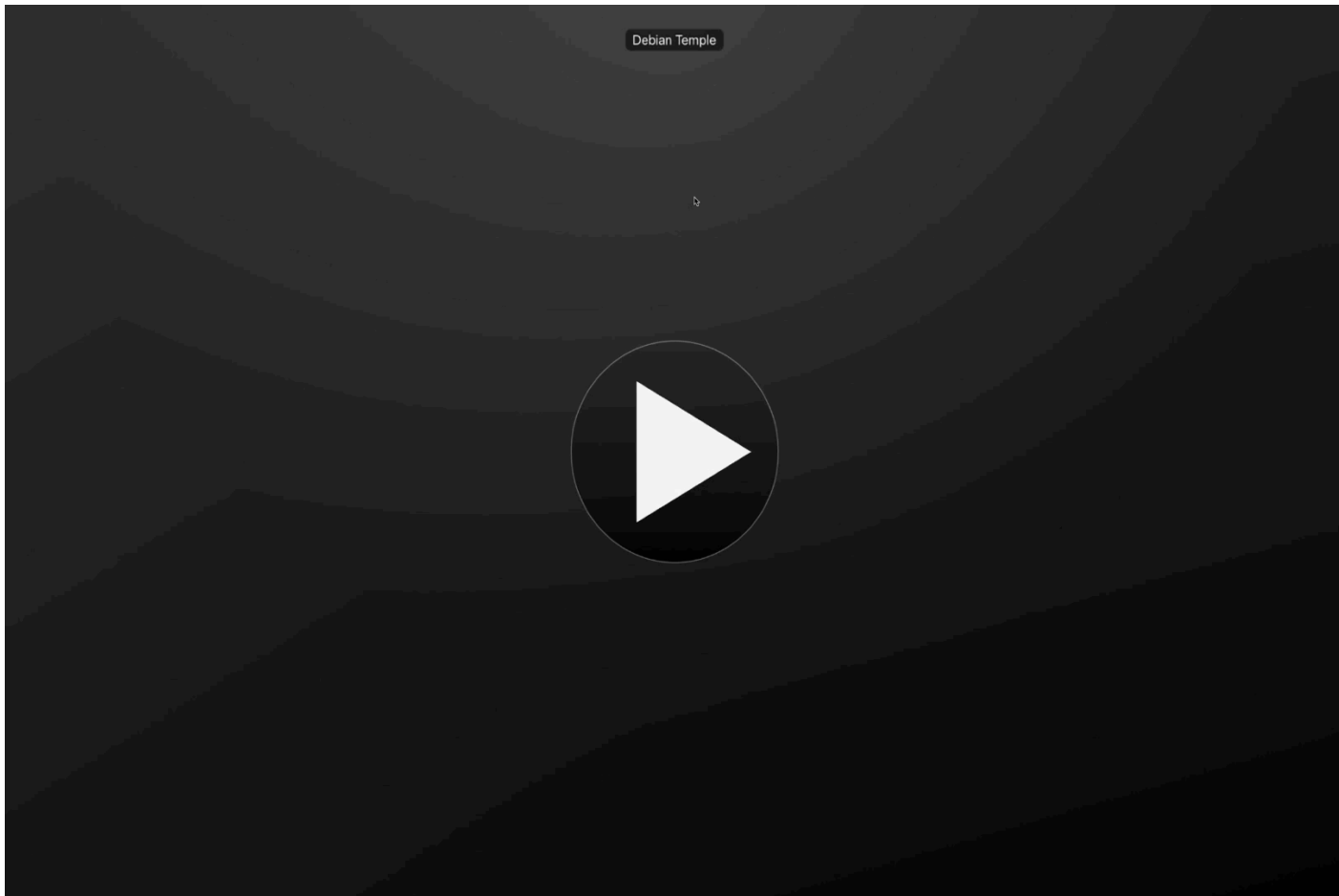
# Setup VM for Kali

7



# Install Kali

8





# Questions From Last Week

9

- Any Questions from last week?
  - What we covered in the last two classes
    - Firewalls
    - Logging

# Questions From Last Week (cont)

10

- Any additional questions?

# Review on-line posts

11

□ A

# Review on-line posts (Cont)

12

- Questions?

# In the News

13

- ❑ WikiLeaks Dumps Docs on CIA's Hacking Tools
  - ❑ WHILE MY SMART TV GENTLY WEEPS
    - <https://krebsonsecurity.com/2017/03/wikileaks-dumps-docs-on-cias-hacking-tools/>
    - Could not resist; I remember saying that I forced my TV into a black-hole via my home router.
    - This one is something to keep up on as further developments hit.
    - Zero-Day was high on the hit list in this thread.
- ❑ Virtual machine escape fetches \$105,000 at Pwn2Own hacking contest [updated]
  - ❑ Drive-by hits MS Edge, Breaks Hypervisor, hits Host
    - <https://arstechnica.com/security/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/>

# In the News (Cont)

14

## ❑ Virtual Machine escape...?

- ❑ <https://arstechnica.com/security/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/>



# In the News (Cont)

15

- Questions?

# Unix/Linux Basics

16

- ❑ How are Windows and Unix different?
- ❑ How are Windows and Unix the same?
- ❑ Directory of interest
- ❑ Commands to learn
- ❑ Tools to have



# Unix/Linux Basics (cont)

17

- How are Windows and Unix different?
  - ▣ Windows
    - Registry
    - Service Database
    - User and Password Database
    - Ipconfig
    - GUI Based
  - ▣ Unix
    - Files - /etc
    - Services = .conf files
    - passwd file
    - Ifconfig
    - Shell based

# Unix/Linux Basics (cont)

18

- How are Windows and Unix the same?
  - Windows
    - Services
    - ACLs
    - GUI and Shell
  - Unix
    - Services
    - ACLs
    - GUI and Shell

# Unix/Linux Basics (cont)

19

- ❑ Directory of interest
  - ❑ /etc – all host specific configuration files
  - ❑ /lib /lib64 – essential share libraries
  - ❑ /var – that contains files to which the system writes data during the course of its operation
  - ❑ /root – root home directory
  - ❑ /tmp – temporary files
  - ❑ /home – User home directories
  - ❑ /proc – Live process information; can change active settings if you do not need to or want to make a permanent change

# Unix/Linux Basics (cont)

20

- ❑ Commands to learn
  - ❑ File management
    - cp – copy
    - mv – move or rename
    - ls – list or directory
    - dd, rsync, tar, find
  - ❑ cat, head, tail, cut, less, sort
  - ❑ dos2unix – remove DOS breaks and convert them to unix stile files. Needed if you create scripts in Windows and prot them over.

# Unix/Linux Basics (cont)

21

- Tools to have
  - ▣ Putty
  - ▣ cygwin

# Unix/Linux Basics (cont)

22

- Questions?

# Scripting

23

- ❑ General scripting
- ❑ Example
- ❑ On-Line Guide: <http://tldp.org/LDP/abs/html/>

# Scripting (cont)

24

- General scripting
  - Writing scripts is a notepad file
    - Write individual steps in a single file
    - Add the scripting engine that should run it
    - chmod to add the execute flag
    - Run the file as any other executable



# Scripting (cont)

25

- Example

```
#!/bin/csh -f
```

```
#
```

```
# this is a comment
```

```
#
```

```
echo "hello world"
```

# Scripting (cont)

26

- Questions?

# Appropriate permissions

27

- ❑ Account Creation
- ❑ Group Creation
- ❑ Group modification
- ❑ Sudo configuration
- ❑ SU lock down
- ❑ Demo

# Appropriate permissions

28

- ❑ Create account
  - ❑ `useradd -m <User Name>`
  - ❑ `passwd <User Name>`
  - ❑ `chsh -s /bin/bash <User Name>`
- ❑ `adduser Andrew sudo`
- ❑ `sudo -s -u <User Name>`
- ❑ `getent group sudo`
- ❑ `deluser Andrew sudo`
- ❑ `/etc/pam.d/su add auth pam_wheel`

# Appropriate permissions (cont)

29

- ❑ Account Creation
  - ❑ `useradd -m <User Name>`
  - ❑ `passwd <User Name>`
  - ❑ `chsh -s /bin/bash <User Name>`

# Appropriate permissions (cont)

30

- ❑ Group Creation
  - ❑ groupadd <Group Name>
  - ❑ groupdel <Group Name>

# Appropriate permissions (cont)

31

- ❑ Group modification
  - ❑ getent group sudo
  - ❑ deluser Andrew sudo

# Appropriate permissions (cont)

32

- ❑ Sudo configuration
  - ❑ visudo – modify what is in the sudo configuration
    - Demo
  - ❑ Change to account or execute commands
    - `sudo -s -u <User Name>`



# Appropriate permissions (cont)

33

- ❑ SU lock down
  - ❑ /etc/pam.d/su add auth pam\_wheel
  - ❑ Demo

# Appropriate permissions (cont)

34

- Demo

# Appropriate permissions (cont)

35

- Questions?

# Assignment 3 Last Minute Questions

36

- ❑ Requirements – Same teams members as before.
  - ❑ A report of the CIS baseline built into a GPO
    - Note: there is a report feature for a GPO to where the setting that have been applied can be exported into a report file; that is the report I'm referring to here.
    - Applied to the same DC Windows 7 pair we have been working from assignment 2.
  - ❑ A video from the team as how this improves our security with faces and voices.
  - ❑ Expand upon the GPO that was created in assignment 2 from 20 settings to what the team feels sufficient to secure Windows 7.
  - ❑ This assignment builds to what is presented to the Pen-Testing class for Assignment 4, so the 4th grade is how well the team does in it's selections from the baseline in assignment 3.
- ❑ Due Date: March 24<sup>th</sup> 11:59pm
  - ❑ Late assignments have a 10% penalty per week.

# Assignment 4 Overview

37

- ❑ Requirements – Same teams members as before
- ❑ Prep your VM
- ❑ Create a Box Location per team
- ❑ Copy to box location
- ❑ Share with Wade's class
- ❑ Get outside assessment of how you did

# Next Week

38

- ❑ Assignment 3 (Due Mar 24<sup>th</sup>)
- ❑ Assignment 4 Overview
- ❑ Configuration management practices
- ❑ Unix/Linux System hardening
- ❑ Baselines
  - ❑ Enabling logging
    - /var/log/messages or /var/log/syslog
  - ❑ Baseline Standards

# Quiz

39

- We can start the Quiz