

MIS 5170

Operating System Security

Week 10

Unix/Linux basics

Tonight's Plan

2

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

Questions From Last Week

3

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

Questions From Last Week (cont)

4

- Any additional questions?

Install Kali

10

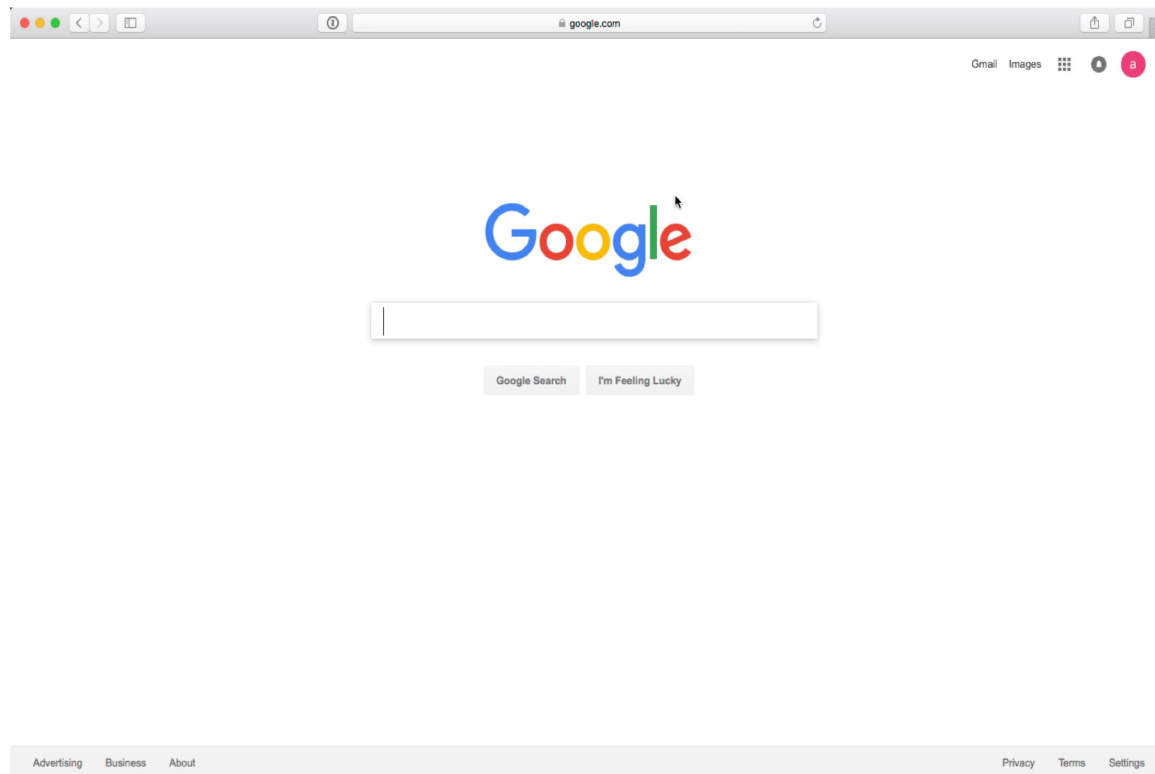
- ❑ Download Kali
- ❑ Setup VM for Kali
- ❑ Install Kali
- ❑ Next Steps

Download Kali

11

□ Download Kali

□ <https://www.kali.org/downloads/>



Verify Download

12

- ❑ Verify Download of Kali
 - ❑ Calculate the sha256sum from download.
 - ❑ MAC
 - `shasum -a 256 kali-linux-2016.2-amd64.iso`
 - ❑ ISO Sha256 sum from Kali download site

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	ISO Torrent	2.9G	2016.2	1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431

Verify Download (cont)

13

- ❑ Verify Download of Kali
 - ❑ Calculate the sha256sum from download.
 - ❑ PowerShell
 - `$Alg = [security.cryptography.hashalgorithm]::create("SHA256")`
 - `$File = [io.file]::readallbytes("<File Name")`
 - `$bytes = $Alg.ComputeHash($File)`
 - `-join ($bytes | foreach {"{0:x2}" -f $_})`
 - ❑ PowerShell 5.0 and up
 - `get-filehash`

```
PS C:\Users\public\downloads> Get-FileHash .\kali-linux-light-2016.2-i386.iso
```

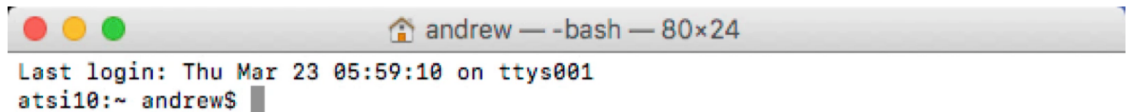
Algorithm	Hash	Path
SHA256	590E6DF2E8E0B4D42BF3DD4E4C7D6ACF24B7262FABDA52A0C6C3B35006DEF295	C:\Users\public\downloads\ka1...

Verify Download (cont)

14

□ Verify Download of Kali

- 1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601
a5d454fa0431

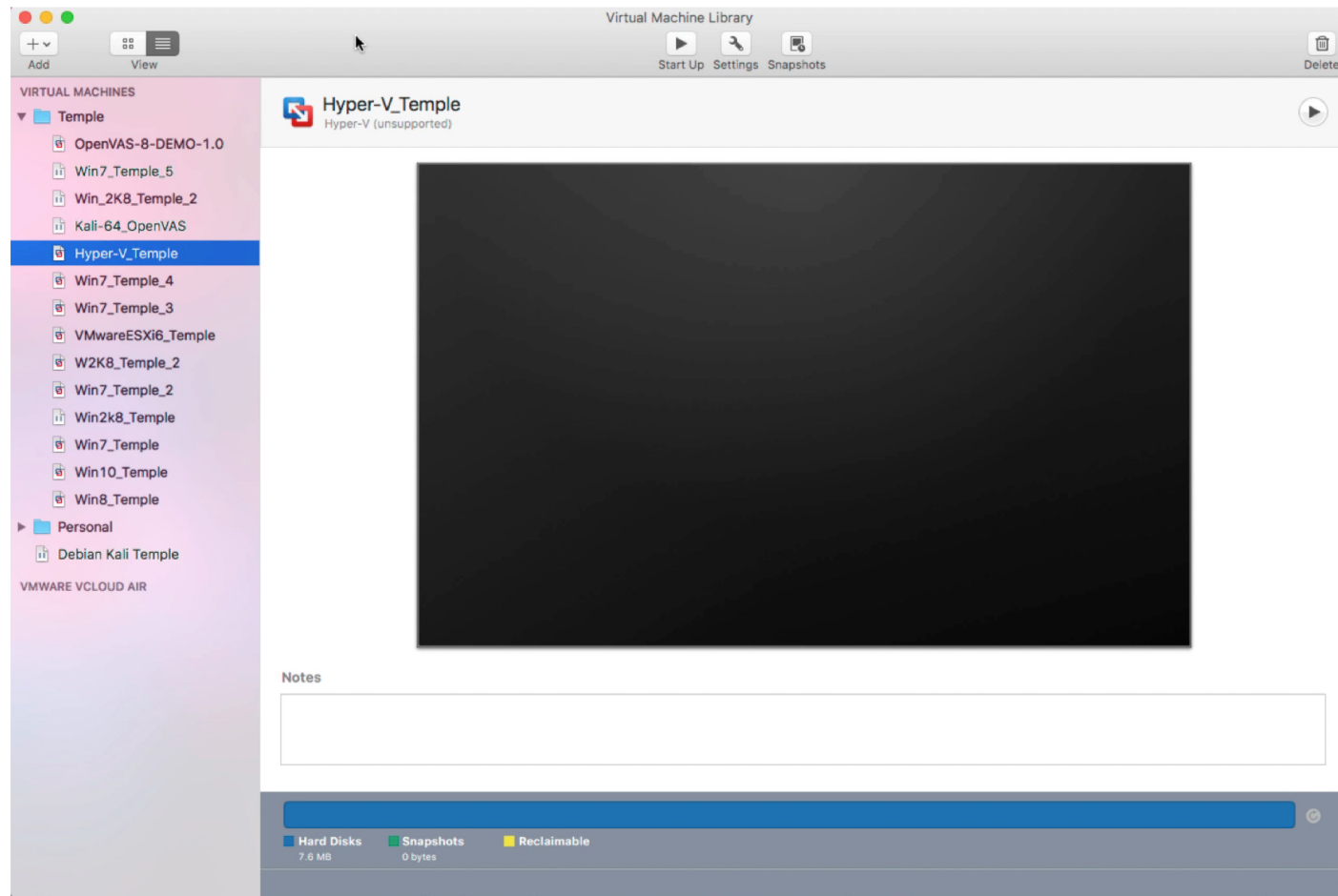
A screenshot of a terminal window with a title bar that reads "andrew — -bash — 80x24". The terminal content shows "Last login: Thu Mar 23 05:59:10 on ttys001" and the prompt "atsi10:~ andrew\$".

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

I

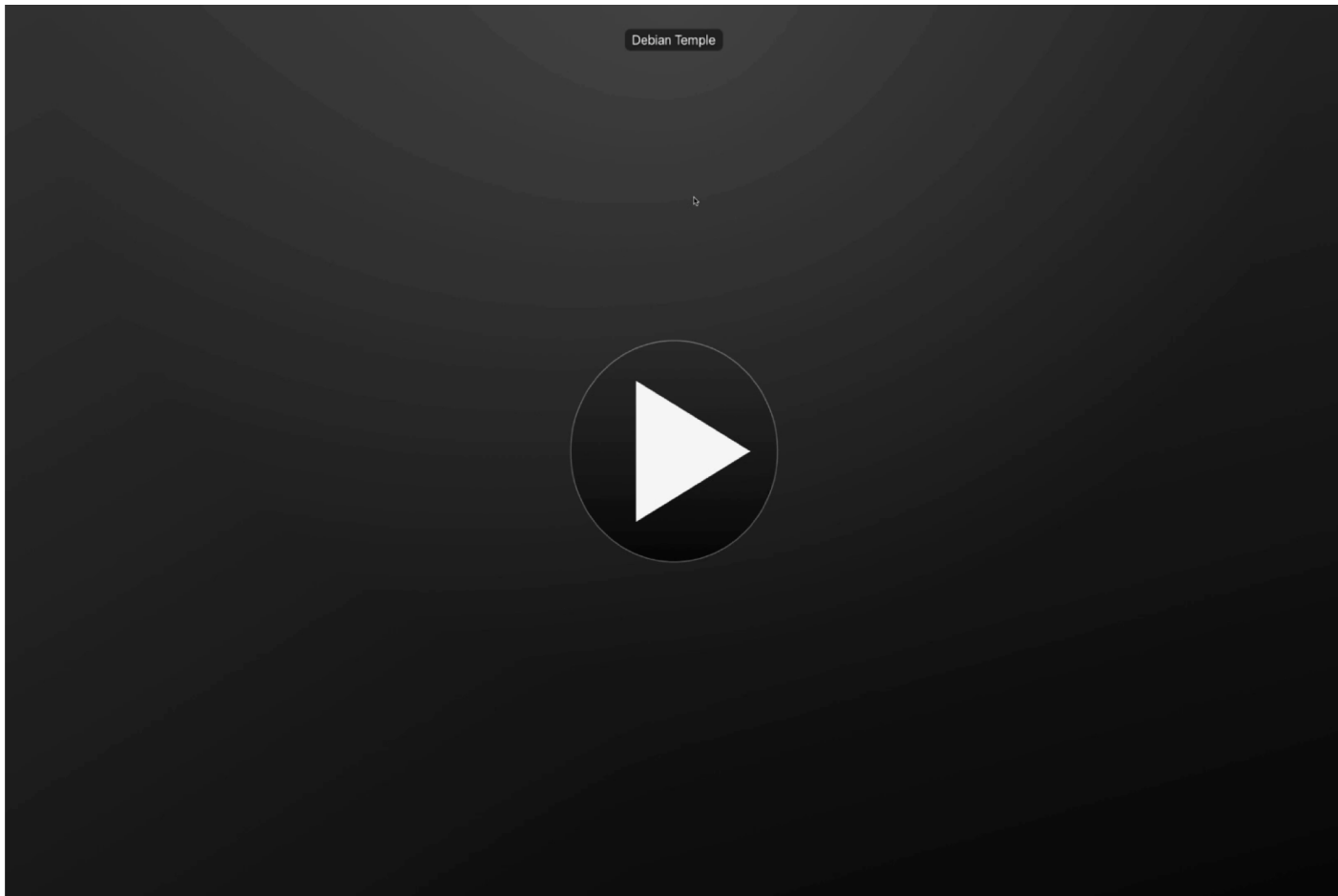
Setup VM for Kali

15



Install Kali

16



Unix/Linux Basics

17

- ❑ 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)

18

- 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)

19

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

Unix/Linux Basics (cont)

20

- ❑ 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)

21

- ❑ 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 port them over.

Unix/Linux Basics (cont)

22

- ❑ Tools to have on Windows
 - ❑ Putty
 - ❑ cygwin

Unix/Linux Basics (cont)

23

- Questions?

Scripting

24

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

Scripting (cont)

25

- 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
 - Writing scripts in vi
 - Demo
 - Help sheet for vi
 - <http://www.lagmonster.org/docs/vi.html>

Scripting (cont)

26

- Example

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

```
#
```

```
# this is a comment
```

```
#
```

```
echo "hello world"
```

Scripting (cont)

27

- Questions?

Appropriate permissions

28

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

Appropriate permissions

29

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

Appropriate permissions (cont)

30

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

Appropriate permissions (cont)

31

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

Appropriate permissions (cont)

32

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

Appropriate permissions (cont)

33

- 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)

34

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

Appropriate permissions (cont)

35

- Demo

Appropriate permissions (cont)

36

- Questions?

Assignment 3 Last Minute Questions

37

- ❑ 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 28th 11:59pm
 - ❑ Late assignments have a 10% penalty per week.

Assignment 4 Overview

38

- ❑ 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

39

- ❑ Assignment 3 (Due Mar 28th)
- ❑ Assignment 4 Overview
- ❑ Configuration management practices
- ❑ Unix/Linux System hardening
- ❑ Baselines
 - ❑ Enabling logging
 - /var/log/messages or /var/log/syslog
 - ❑ Baseline Standards

Quiz

40

- We can start the Quiz