Cyber Security Technologies

Session 1a – Course Overview

Shawn Davis
ITMS 448 – Spring 2016

Slides may contain original content from Davis, S. and Lidinsky, W.

Course Instructor

- Shawn Davis (GWAPT, GCFE, GCIH, Sec+, Net+, A+)
- Industry Experience:
  - Director of Digital Forensics (Current)
  - Computer Forensics Investigator
  - Information Protection Specialist
  - Technology Consultant
  - Pre-sales Engineer

Aside from Technology…

Introductions

- Student Introductions:
  - Name
  - Where you work and what you do there
  - What experience you currently have with information security
    - Systems & network security, pen-testing, forensics, malware analysis, etc.
  - Something fun you did over break

ITMS 448 Course Content

- The main components of this course include:
  - Lectures of important Information Security topics and in-class hands-on labs
  - Homework (which includes hands-on labs)
  - Individual Project

Prerequisite Knowledge

- In order to succeed in this course, you should already have a good working knowledge of:
  - The internal operation and use of the Internet
  - Windows and Linux operating systems
  - Some ability to write code or scripts

Prerequisite Knowledge (Cont.)

- If you are lacking in the above areas, you may need to put in additional effort to succeed in the course.

Seating

- Take note of the ID on top of your physical computer
- You will be sitting in these same seats for the rest of the semester as the disk in your computer is now assigned to you
- Your disk is not guaranteed to persistently save your data for the entire semester though. Please save anything you need to keep to personal media or to a cloud drive

Individual Project

- This project is based on defending a Linux or Windows system service
- Next week I will email each of you a specific system service
- If there is a specific service you are particularly interested in learning about, have access to, and would like me to consider assigning you, please email me with it before 1/18

Individual Project

- Over the semester you will be responsible for:
  - Installing the service and learning how it functions
  - Understanding the default configuration options
  - Learning multiple methods to attack the service
    - Changing default configuration options, use of other services or hardware, etc.
  - Learning how to harden the service to defend against attacks

Individual Project Timeline

- You should have your service installed, functioning, and understand the default options before class on Feb 15th
- You should understand and be able to demonstrate all of the methods to attack the service before class on Mar 21st
- You should be able to describe your methods of hardening the service before class on Apr 11th

Individual Project Deliverables

- Each student will turn in the following to me before class on April 11th
- 5-10 PowerPoint slides explaining:
  - what your service does
  - the default configuration options
  - your attack methods
  - your methods to harden the service to defend against attack
- Short video (1 minute) showing at least one example of your running server being attacked and then resisting that same attack after being hardened.

Individual Project Deliverables

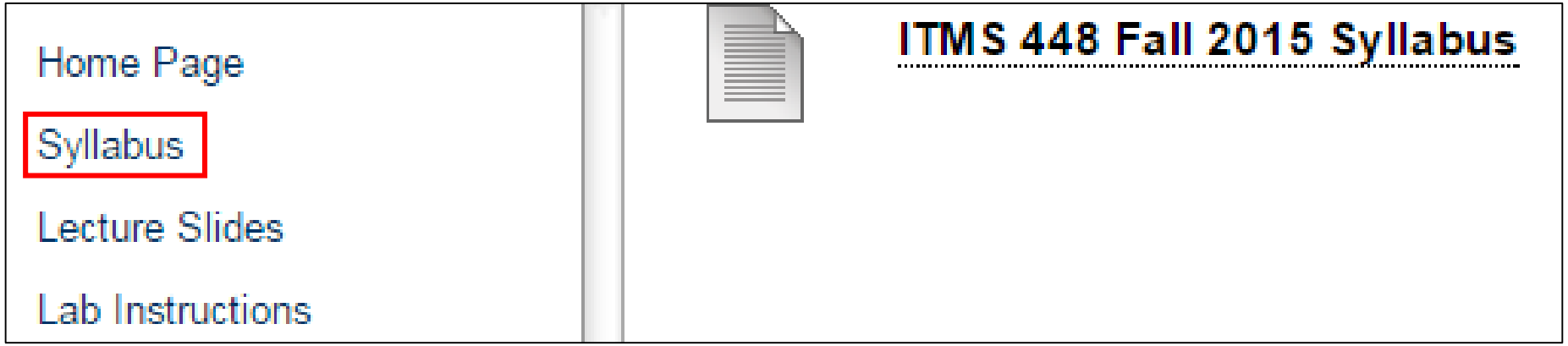
- I will review the PowerPoints and videos shortly after April 11th and will provide feedback for any needed changes
- On Apr 25th, each student will present their PowerPoint and video to the class

Blackboard

- Most everything related to this course is posted on Blackboard
- The following screenshots shown in this slide deck are of Blackboard

Course Syllabus

- …is posted on Blackboard
- You are responsible for reading and understanding the **entire** syllabus
- If you do not understand any part of the syllabus please let me know right away



Course Sessions

- Each class will typically be broken up between lecture and labs
- Consult the course syllabus before each class session to view that day's topic schedule

Course Syllabus Topic Schedule

Schedule of Topics:

Week	Date	Topic
1	Jan 11	Course Intro, RADISH, Security Overview
2	Jan 18	**Martin Luther King, Jr. Day - No Classes**
3	Jan 25	Malware Overview & Exploit Kits
4	Feb 1	Malware Analysis

Blackboard

- You will submit all homework/labs deliverables to Bb before their assigned due dates
- After each lecture (and often beforehand) a pdf of the slides will be uploaded to Bb in the “Lecture Slides” folder
- Your grades and feedback can be viewed in Bb under Tools / “My Grades”

Attendance/Class Participation

- Worth 10% of your course grade
- **Class Participation:**
  - Speak up and don't be afraid to ask and answer questions!
  - There are no dumb questions or answers in here
  - Sitting here the entire term and not participating in discussion during lectures will affect your grade

Attendance/Class Participation (Cont.)

- **Attendance**
  - If you cannot attend a class, please email me prior to class with the reason
  - You are allowed two excused absences over the course of the semester without penalty
  - If you do not email me prior to class, the absence is considered unexcused
  - Attendance is mandatory for exams and for the delivery of your project presentation

Course Text

- There is no required text book for this course
- Supplemental online reading will be assigned throughout the semester

Homework

- Homework will generally be due prior to midnight on the second Sunday following the class in which it was assigned
  - Example:
    - Today is Monday, Jan 11th and a homework assignment will be assigned
    - The assigned homework must be submitted to Bb before midnight on Sunday, January 24th
  - Exceptions may occur before an exam or at the end of the semester.

Homework (Cont.)

- An almost two week due date affords students:
  - The opportunity to try the assignment before the next class session and get help if needed.
  - The opportunity to complete an assignment on time even if they are busy, sick, have issues with RADISH, etc.
- Due to this:
  - Students are allowed only **one** late homework submission during the semester and it must be turned in within 48 hours of the original due date
  - **No other late homework will not be accepted**

Homework (Cont.)

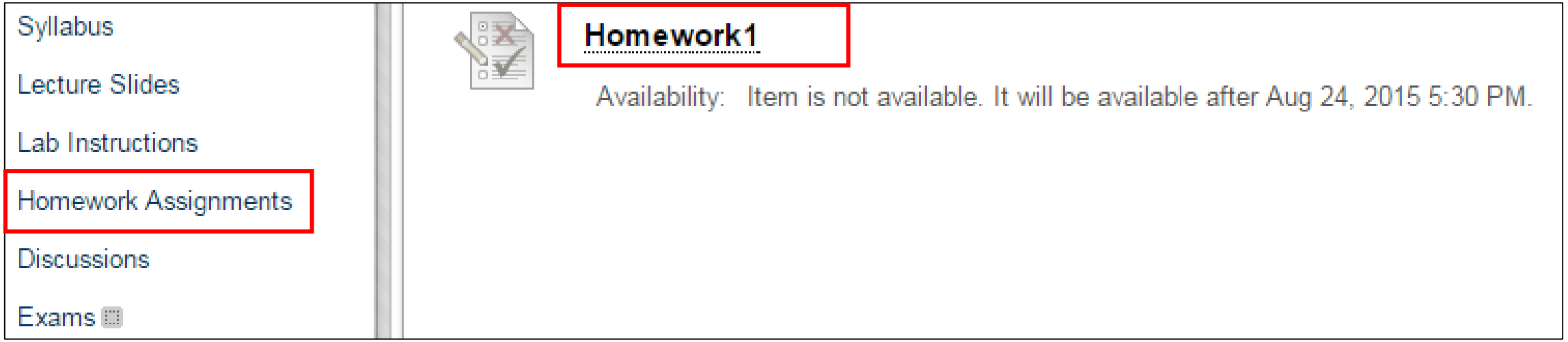
- Please don't wait until the last day to start on your homework
- Start on your homework as early as possible so that you may contact me (with any homework questions) or Dawid (for any issues connecting to RADISH) well before the due date

Homework (Cont.)

- Homework assignments are not listed in the syllabus.

- Homework and their due date are listed on Blackboard as well as the end of each lecture slide deck. You are responsible for checking the "Homework Assignments" folder.

Homework Process Example – Week 1



Homework Process Example – Week 1

INSTRUCTIONS

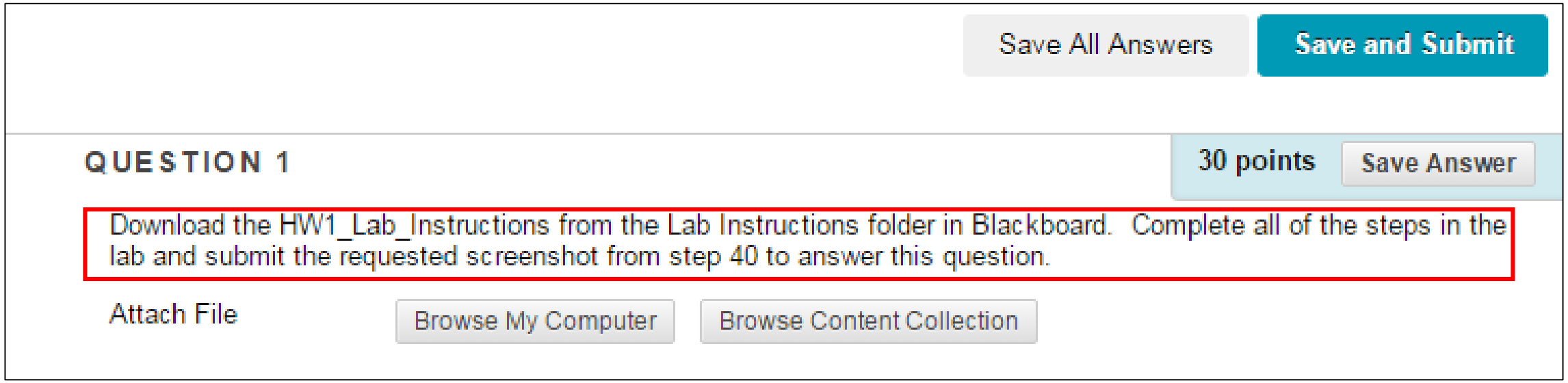
Force Completion	This test can be saved and resumed later.
Due Date	This Test is due on January 24, 2016 11:59:00 PM CST.Test cannot be started past this date.

Click **Begin** to start: Homework1. Click **Cancel** to go back.
You will be previewing this assessment and your results will not be recorded.

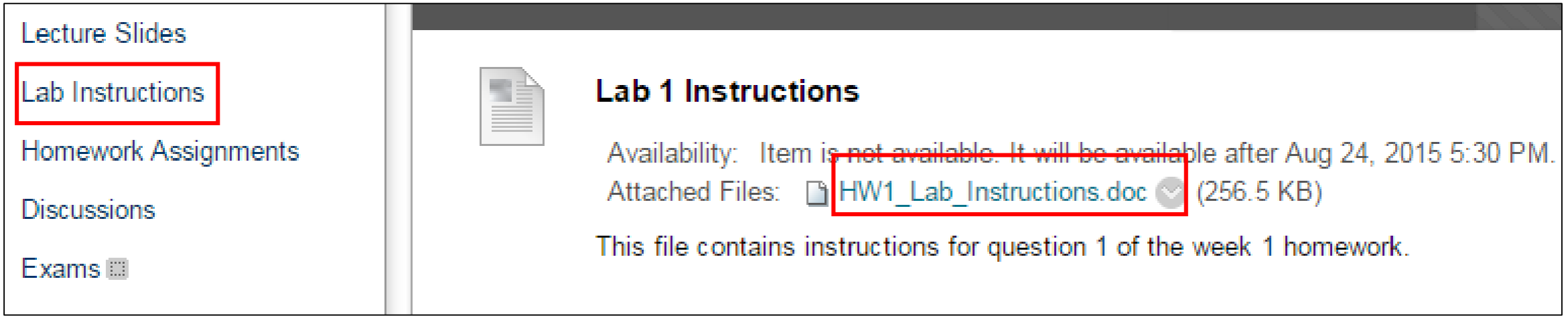
Click Begin to start. Click Cancel to quit.

Cancel Begin

Homework Process Example – Week 1



Homework Process Example – Week 1



Homework Process Example – Week 1

HW1_Lab_Instructions

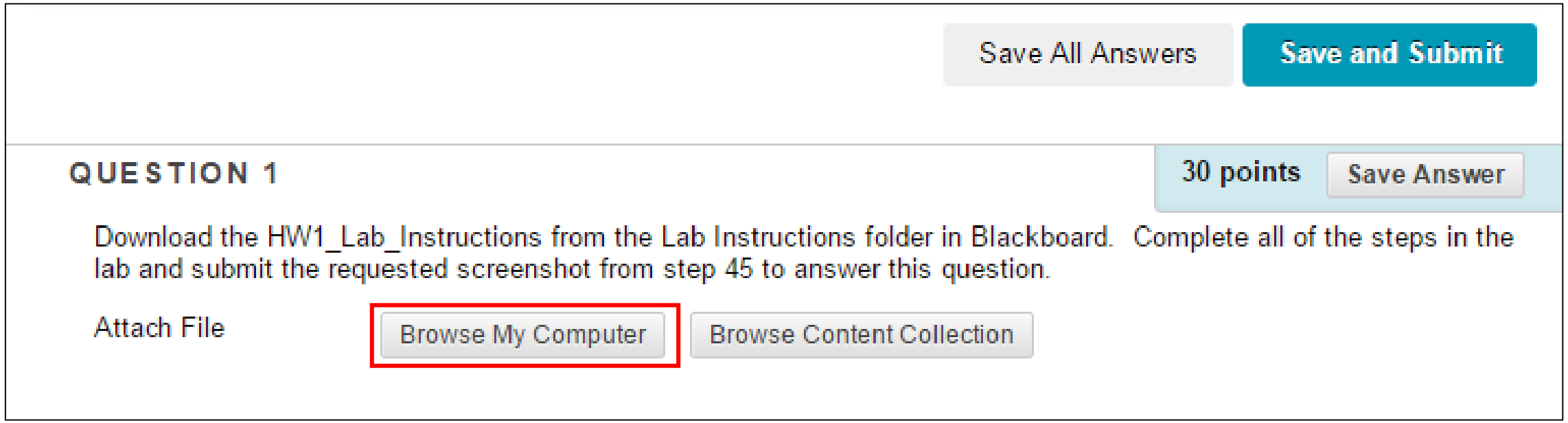
In class, we used SET to use a pre-existing Google template to capture user credentials. In this lab, we will take that concept further and use SET to clone Chase Bank's website and use a Cross Site Scripting (XSS) attack by embedding a BeEF Javascript hook into it. This hook will allow the attacker to use BeEF in order to take control of the user's browser to capture credentials and also perform additional actions.

1) Connect to your Windows 8 Student VM from home via Radish using the VMware View Horizon client. Enter the logon credentials you received from Dawid.
2) Open your Kali Linux Machine with the TightVNC Icon on the Window's Desktop.

Homework Process Example – Week 1

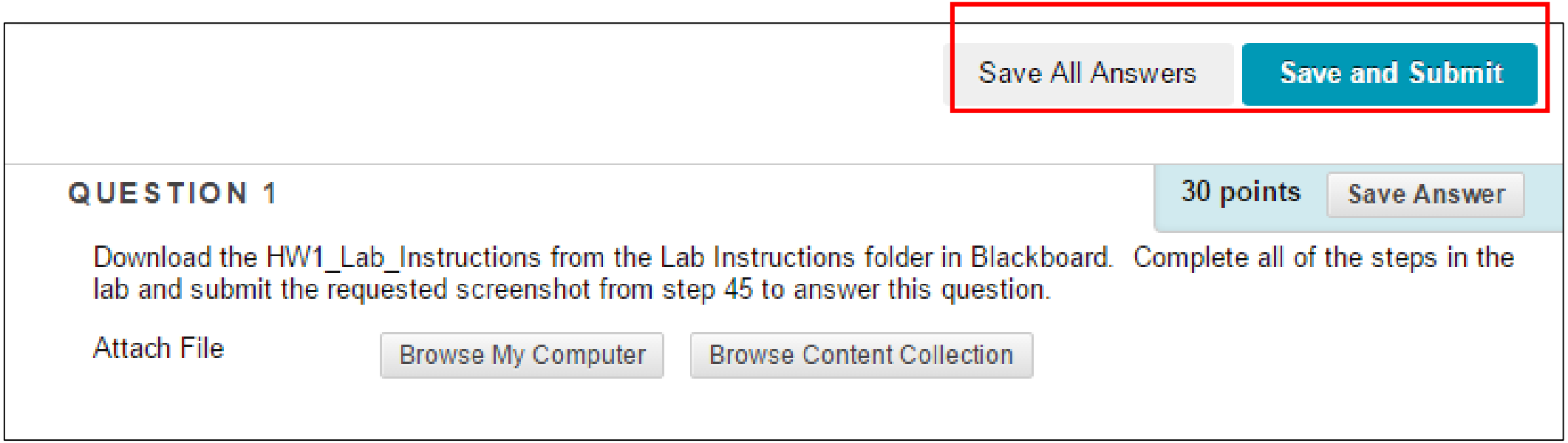
45) ***At this point, take a screen capture of the Log in BeEF that you viewed in step 44 showing your username and password entered in step 43. Use the Windows Snipping tool and save the screen capture as a jpg file. You will upload this file to answer question 1 of Homework1 on Blackboard.***

Homework Process Example – Week 1



Homework Process Example – Week 1

- Do NOT click "Save and Submit" until you are ready to hand in the homework for grading.
- Click "Save Answer" or "Save All Answers" so that you can pick up where you left off later.



Homework Process

- Other Homework questions may include:
  - Essay
  - Short Answer
  - Multiple Choice
  - Multiple Answer
  - True/False
  - Other Question Types

Homework

- Homework should be completed individually by each student
- Homework should be in your own words
- While you may collaborate on some of the in-class Labs, do not collaborate on:
  - Homework Labs and Assignments
  - Exams

RADISH

- Hosted VM infrastructure on Rice Campus
- Will be used for:
  - In-class labs from PH218
  - Homework labs from your personal computers
- Consists of Windows 8.1 VM and Kali Linux VM (and 1-2 others later)

Open Lab Hours

- If you have issues with your personal computer, you can access RADISH from the TS2033 lab during open lab hours when class is not in session there
- Open Lab hours in TS2033 start 1/22 and can be found on this doc where it says “Open Lab”
  - https://calendar.google.com/calendar/b/2/embed?src=iit.edu_fnlop4dno8fcm7jsfvajh7anjg@group.calendar.google.com&ctz=America/Chicago&pli=1
- There are **no** open lab hours in PH218

Open Lab Hours (Cont.)

- The TS2033 lab drives will not be persistent for storage so please save anything you need to keep to personal media or a cloud drive

Sharing of Course Content is Prohibited

- Do NOT upload to the internet (outside of Bb) or share any of the course materials such as:
  - Homework questions and your answers
  - Lab instructions
  - Exams
  - Lecture Slides

Lectures

- You are encouraged to download copies of the course lecture slides for your own personal use
- Lectures will generally consist of:
  - Slides and Discussion
  - Slides and Lab In-Class Lab Walkthrough

Plagiarism – Homework

- You should not be copying other people's words into your homework.
  - Example: Do copy a sentence or paragraph from Wikipedia and turn it in as your answer
- You should not be using other people's code for your homework.

Plagiarism Consequences

- All assignments are automatically run through a plagiarism checker.
- Any plagiarism found will result in a zero for that assignment as well as an academic dishonesty report filed with the college.

Grade Weighting

- Homework Assignments – 50%
- Individual Project – 5%
- Attendance/Class Participation – 10%
- Midterm Exam – 15%
- Final Exam – 20%

Questions???

Next

- Radish – Slide Deck B