

---

# AC 2012-4107: USING AMAZON EC2 IN COMPUTER AND NETWORK SECURITY LAB EXERCISES: DESIGN, RESULTS, AND ANALYSIS

## **Dr. Chuan Yue, University of Colorado, Colorado Springs**

Chuan Yue is an Assistant Professor of computer science at the University of Colorado, Colorado Springs (UCCS). His current research focuses on web browsing security and collaborative browsing. His broad research interests include computer and information security, web-based systems, human-computer interaction, collaborative computing, distributed and parallel computing, and cloud computing. He received his B.E. and M.E. degrees in computer science from the Xidian University, China, in 1996 and 1999, respectively, and his Ph.D. in computer science from the College of William and Mary in 2010. He worked as a member of technical staff at Bell Labs China, Lucent Technologies, for four years from 1999 to 2003, mainly on the development of a web-based distributed service management system for an intelligent network.

## **Dr. Weiyong Zhu, Metropolitan State College of Denver**

Weiyong Zhu received a Ph.D. in electrical and computer engineering from Old Dominion University, Norfolk, Va., in Aug. 2006, a M.S. in communication and information engineering from Huazhong University of Science and Technology, Wuhan, China, in June 1999, and a B.S. in biomedical electronic engineering from Xi'an Jiaotong University, Xi'an, China, in July 1996. She worked as a Software Engineer in Bell Labs China at Lucent Technologies from July 1999 to Jan. 2003. She had been an Assistant Professor in Hampton University from Aug. 2006 to July 2011. She joined Metropolitan State College of Denver in Aug. 2011. Her career has been distinguished by a series of awards such as the in the Provost Teaching Innovation Award in April 2010, the First Place Graduate Research Award at Global Challenges, Local Solutions: Annual Research Expo in Norfolk, Va., in April 2006, the University Dissertation Fellowship in Academic Year 20052006, the ECE Ph.D. Research Assistant Award in 2004, the member of Bell Labs President's Gold Winner Team Award in 2000, and the University Outstanding Thesis Award in 1999.

## **Mr. Gregory Lynn Williams, University of Colorado, Colorado Springs**

Gregory Williams is the Information Technology Security Principal for the University of Colorado, Colorado Springs, and is currently working toward his master's of engineering degree in information assurance also from the University of Colorado, Colorado Springs. He has a passion for learning for not only information security concepts and theory, but also current real world technology and zero-day threat models. His passion for education has lead him to help others understand why information security is important and what we can do to defend our information.

## **Prof. Edward Chow, University of Colorado, Colorado Springs**

C. Edward Chow is professor of computer science at the University of Colorado, Colorado Springs. He received his Ph.D. from the University of Texas, Austin. His research aims at improving the security, reliability, and performance of network systems. He has two U.S. patents on distributed network restoration and survivable architecture. He recently developed an efficient internet security (IPSec) protocol that significantly improves the performance and security of online storage systems. In an AFOSR-NISSC sponsored project, a secure information sharing system was developed for setting up secure information infrastructure which is based on attribute certificate to coordinate multiple agencies task forces. He is the Principal Investigator of an international collaboration project that involves Taipei National Art University, UCCS, and Denver Children Hospital, using Laban dance notation, computer animation, and a wireless sensor-based human motion tracking system to improve rehab patient care. He just received an Air Force SBIR grant to develop games for accelerating the learning of techniques against insider attacks. He organized the UC Lion team to compete in 2006-2010 international Capture the Flag cyber security exercises held in December.

# Using Amazon EC2 in Computer and Network Security Lab Exercises: Design, Results, and Analysis

## Abstract

Cloud computing is a significant trend in computing. In this paper, we present our experience in using Amazon EC2 (Amazon Elastic Compute Cloud) as the platform to support the hands-on lab exercises of a computer and network security course. In this course, each student is required to perform four realistic lab exercises using Amazon EC2: an IDS (Intrusion Detection System) lab exercise, a Linux firewall lab exercise, a Web security lab exercise, and a software vulnerability exploitation lab exercise. Hosting these security lab exercises in the cloud brings us two main benefits. One is that we can better prepare our students for their future careers in a cloud computing world. The other is that we can effectively address the resource limitation of our existing lab environments and meanwhile ease the burden on our IT professionals who need to take care of the needs of many courses and maintain the existing infrastructure for college operations. Using Amazon EC2 in particular, we can take advantage of its reliability, availability, robustness, accessibility, security, and uniformity. Through the survey answered by our students, we found that the majority of our students are in favor of learning and using such a leading cloud computing platform, and a common opinion among students is that Amazon EC2 is easy to learn and convenient to use. We describe the setup of our EC2 environment and the design of those four lab exercises. We also detail the survey results and analyze the implications of those results. The experience presented in this paper is valuable for our faculty members to move more lab exercises into the cloud. We believe our experience is also valuable to other educators who plan to use cloud computing services such as Amazon EC2 in their computer science and engineering courses. The link to our complete lab manuals and instructions is listed at the end of the bibliographic section.

## 1. Introduction

There is no doubt that cloud computing has become a reality. People talk about it, spend money on it, and gain substantial benefit from it. In response to this significant trend in computing, our colleges encourage faculty members to use cloud computing services such as AWS (Amazon Web Services)<sup>[1]</sup> in teaching computer science and engineering courses. On the one hand, we can better prepare our students for their future careers in a cloud computing world; on the other hand, we can effectively address the resource limitation of our existing lab environments and meanwhile ease the burden on our IT professionals who need to take care of the needs of many courses and maintain the existing infrastructure for college operations.

Hands-on lab exercises play an important role in teaching a computer and network security course because they can help students apply basic security principles and techniques to the protection of real world computer and network systems. Our computer and network security course is a three-credit lecture course. In this course, in addition to attending lectures, doing homework assignments, presenting research papers, conducting course projects, students will

also work individually on four lab exercises outside the class hours: an IDS (Intrusion Detection System) lab exercise, a Linux firewall lab exercise, a Web security lab exercise, and a software vulnerability exploitation lab exercise. Students are also encouraged to join our UC Lions team to attend the annual UCSB International Capture The Flag (iCTF) security competition<sup>[22, 23]</sup>.

In Fall 2011, our students used Amazon EC2 (Elastic Compute Cloud)<sup>[21]</sup> as the platform to work on the four lab exercises of our computer and network security course. There are 28 students in the class. At the beginning of the semester, the instructor Dr. Chuan Yue was awarded an AWS Teaching Grant<sup>[3]</sup> from Amazon to use the AWS cloud infrastructure in teaching. The total credit awarded to the instructor is \$3,600. At the end of the semester when students completed all the four lab exercises, \$3,311 remained on the instructor's AWS account. Hence, 28 students, one instructor, and one teaching assistant have amazingly used only \$289 for four lab exercises in a semester, much less than the originally expected cost. At the end of each lab exercise, a survey was given to students to obtain insight on students' perception of using Amazon EC2 for hands-on security lab exercises. According to the survey results, the average number of hours worked on each lab exercise varies between 7.0 hours and 14.5 hours as shown in Figure 7. These results indicate that Amazon EC2 can be cost-effectively used for hosting hands-on lab exercises.

In this paper, we present our experience in three aspects. In Section 2, we introduce the features of Amazon EC2 that are relevant to our lab exercises, the advantages of using EC2 in our lab exercises, and the details of setting up and using EC2 to support our lab exercises. In Section 3, we briefly describe the design of our four lab exercises. In Section 4, we present and analyze the survey results. The survey includes closed-ended questions regarding students' ranking on their EC2 and Linux skills, their opinions on the difficulty of each lab exercise, their opinions on the convenience of using EC2 to perform each lab exercise, and their willingness to use EC2 for lab exercises in this and other computer science and engineering courses. The survey also includes open-ended questions regarding students' other comments and suggestions. In Section 5, we briefly present the student learning and instructor evaluation results. Finally, in Section 6, we conclude the paper.

The experience presented in this paper is valuable for our faculty members to move more lab exercises into the cloud. Other educators have also designed hands-on lab exercises in their computer and network security related courses such as in<sup>[24, 25, 26, 27]</sup>. However, to the best of our knowledge, our course is the first that uses the Amazon EC2 cloud computing infrastructure to host security lab exercises. We believe our experience is also valuable to other educators who plan to use cloud computing services such as Amazon EC2 in their computer science and engineering courses. Our discussions regarding the management of students' AWS accounts and EC2 instances could also be valuable for cloud computing service providers to add new features or improve existing features.

## 2. Use of Amazon EC2

“Amazon EC2 is a Web service that provides resizable compute capacity in the cloud<sup>[2]</sup>.” It provides a true virtual computing environment that can be created and managed by users via

Web service interfaces. Such a virtual environment is used by our students as the platform to accomplish all the four lab exercises designed for our computer and network security course.

## 2.1 Relevant Features and Advantages of Amazon EC2

To use Amazon EC2, a user first selects or creates an AMI (Amazon Machine Image)<sup>[4]</sup> containing the operating system, applications, libraries, data, and associated configuration settings<sup>[2]</sup>. Then the user creates and starts one or multiple EC2 instances using this AMI. Each EC2 instance is a virtual machine that can be stopped and restarted while retaining all the data. The current capacity of EC2 instances ranges from 32-bit Micro Instances (613 MB of memory, one EC2 compute unit, and zero local instance storage) to 64-bit Extra Large Cluster Compute Instances (60.5 GB of memory, 88 EC2 compute units, and 3370 GB of local instance storage)<sup>[8]</sup>. Each EC2 compute unit provides the equivalent capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor<sup>[2]</sup>. The charge to an AWS account depends on the compute capacity that is actually consumed. For example, in terms of the EC2 instances, the charge depends on the type and capacity of the EC2 instances and the running time of those instances.

Typically, the operating system on an AMI can be configured as a Windows Server or one of a variety of Linux operating systems such as Red Hat, SUSE, Ubuntu, etc. Different AMIs with the same type of operating system can be configured to contain different sets of software including Web servers such as Apache, databases such as MySQL, application development environments such as JBoss Enterprise Application Platform, and so on.

Using Amazon EC2 to host our computer and network security lab exercises, we can take advantage of its reliability, availability, robustness, accessibility, security, and uniformity. Guaranteed by Amazon's cloud infrastructure, EC2 instances are highly reliable, available, and robust. Due to the nature of cloud computing, students can access EC2 instances anytime and anywhere simply using a regular Web browser and an SSH (Secure Shell)<sup>[5]</sup> terminal. Students can easily restart or stop the same EC2 instances whenever necessary. In our security lab exercises, students install and analyze vulnerable services and applications and often perform tasks at the system level as root users. By hosting those lab exercises in the well-protected EC2 environment<sup>[6]</sup>, we eliminate the potential security risks on our campus networks and systems. To provide a uniform platform, the instructor can simply create or specify an AMI<sup>[4]</sup> that is configured according to the needs of a lab exercise. Then each student uses this AMI to create his or her own EC2 instance. All the students are able to work on identical but independent virtual machines for their lab exercises. Students also have the complete control and *root* access to their EC2 instances. Mainly due to security concerns, such a root access to computers is difficult to be supported in a regular departmental computer lab where a virtual machine environment has not been used or well managed. Moreover, even if a student messes up an EC2 instance, the student can simply and quickly start over by creating a new one.

## 2.2 Setup and Use of Amazon EC2 Instances for Our Lab Exercises

Like other cloud service providers, Amazon uses the pay-as-you-go pricing model. In our lab exercises, unless explicitly specified, each student only needs to create and run one *micro*<sup>[8]</sup> EC2 instance. A student is also advised to stop the EC2 instance whenever he or she does not use it.

This section presents how to set up and use an EC2 instance to work on the tasks in our lab exercises.

In our practice, we applied all the credits of the AWS Teaching Grant to the instructor's central AWS account and used the AWS Identity and Access Management (IAM)<sup>[7]</sup> Web service to create and manage student user accounts. With this approach, only the instructor needs to use a credit card to activate his AWS account, and the key advantage is that the instructor can easily monitor and manage the use of EC2 instances in all the lab exercises. We did not take another approach, which is to ask students to activate and manage their own AWS accounts.

The setup and use of an EC2 instance can be summarized as below from an instructor's perspective and a student's perspective.

**An instructor** logs into the central AWS account to perform the following steps:

- (1) Use the AWS Identity and Access Management (IAM)<sup>[7]</sup> Web service to create user groups and users. In our case, we created one Student Group and one Administrator Group. We created an AWS account for each student, and assigned all the student users to the Student Group. We also created two test AWS accounts and assigned them to the Student Group. These two test accounts were used by the instructor and the teaching assistant to experiment with the EC2 environment as student users. We created two more AWS accounts and assigned them to the Administrator Group. These two administrator accounts were used by the instructor and the teaching assistant to perform regular EC2 instance management tasks. We created an access control policy as shown in Figure 1 and applied it to the Student Group. This policy allows students to flexibly perform all the four lab exercises with only the necessary permissions. We also used IAM<sup>[7]</sup> to create a unique password for each user.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:CreateKeyPair",
        "ec2:CreateTags",
        "ec2:DescribeTags"
      ],
      "Resource": "*"
    }
  ]
}
```

Figure 1. Access control policy assigned to the Student Group

- (2) Create an AWS account alias (e.g. cs5910uccs) so that all the users can use a simple sign-in URL (e.g., <https://cs5910uccs.signin.aws.amazon.com/console>) to log into the AWS Management Console<sup>[9]</sup> to manage their EC2 instances.
- (3) Create or select AMIs<sup>[4]</sup> to be used by the class for lab exercises. In our case, we simply selected an existing AMI named *ami-8614e3ef* for students to use. The operating system of this AMI is Ubuntu Linux 10.04. This AMI also includes Apache v2.2.14, PHP v5.3.2, and MySQL v5.1.41, which are needed by the tasks in our security lab exercises and represent a typical Linux Web server. Based on an existing Microsoft Windows 2008 AMI named *ami-75b5791c*, we also created a new AMI named *ami-132be27a* to contain an old version Firefox (version 3.6.16) Web browser with vulnerabilities. This new Windows AMI is used in our Lab exercise 4 (i.e., software vulnerability exploitation). It is important to note that cares should be taken when selecting public AMIs because they may be vulnerable to security risks such as unauthorized access, malware infections, and loss of sensitive information<sup>[21]</sup>. We performed a preliminary security investigation on the two AMIs before we chose them, but we suggest readers to perform a more in-depth security analysis<sup>[21]</sup> of these or other public AMIs before selecting them.
- (4) Create and configure a security group to restrict the inbound traffic to EC2 instances. This security group defines an external firewall with the rules enforced by the Amazon EC2 infrastructure. Any EC2 instance associated with this security group will be protected by such an external firewall. In our case, we defined a security group that only enabled SSH and HTTP traffic in our Lab exercise 1 (i.e., IDS). We did that because we want to well protect students' EC2 instances when our students just began to become familiar with the EC2 environment. In the following three lab exercises, we modified our security group and enabled inbound traffic from any source IP address and port number to any TCP or UDP port of an EC2 instance. We made this modification because in our Lab exercise 2 (i.e., Linux firewall), we need to expose students' EC2 instances to any type of inbound traffic so that each student can define the internal firewall to protect his or her own EC2 instance. In addition, TCP ports 445 and 8834 need be opened in our Lab exercise 4 (i.e., software vulnerability exploitation) which is based on the Nessus<sup>[16]</sup> vulnerability scanner. Note that any change made to the security group will be automatically applied to all the associated EC2 instances; therefore, students do no need to re-configure anything. This security group feature of Amazon EC2 is very useful and convenient for us to flexibly design and deploy our security lab exercises.

**A student** logs into his or her AWS account to perform the following steps (more details at<sup>[33]</sup>):

- (1) Use a browser and the AWS account to log into the AWS Management Console (e.g., <https://cs5910uccs.signin.aws.amazon.com/console>).
- (2) Configure an EC2 instance based on an AMI (e.g. *ami-8614e3ef*).
- (3) Generate and save a key pair that will be used later for securely connecting to the EC2 instance.
- (4) Associate a security group created by the instructor to the EC2 instance.
- (5) Launch the EC2 instance.
- (6) Connect to the EC2 instance (via its public DNS name) from an SSH<sup>[5]</sup> terminal.

- (7) Work on a lab exercise by using the EC2 instance via the SSH terminal.
- (8) Stop the instance if the user will not use the EC2 instance for a period of time, and start it whenever needed.

We now provide more details about these eight steps. The first five steps only need be performed once by a user for an EC2 instance. In our case, each student reuses the same instance for all the four lab exercises. Figure 2 is a snapshot of the AWS Management Console when a user reviews the configuration of his or her EC2 instance right before launching it at step 5. One *micro* instance<sup>[8]</sup> is powerful enough to support all the tasks in each of our four lab exercises. To minimize the charge to the instructor's AWS account, we asked each student to start only one micro EC2 instance at any time. Each student is also required to specify at least one tag for his or her EC2 instance, and the tag should contain the student's AWS account name. Therefore, the instructor, the teaching assistant, and students can easily search and observe each individual EC2 instance.

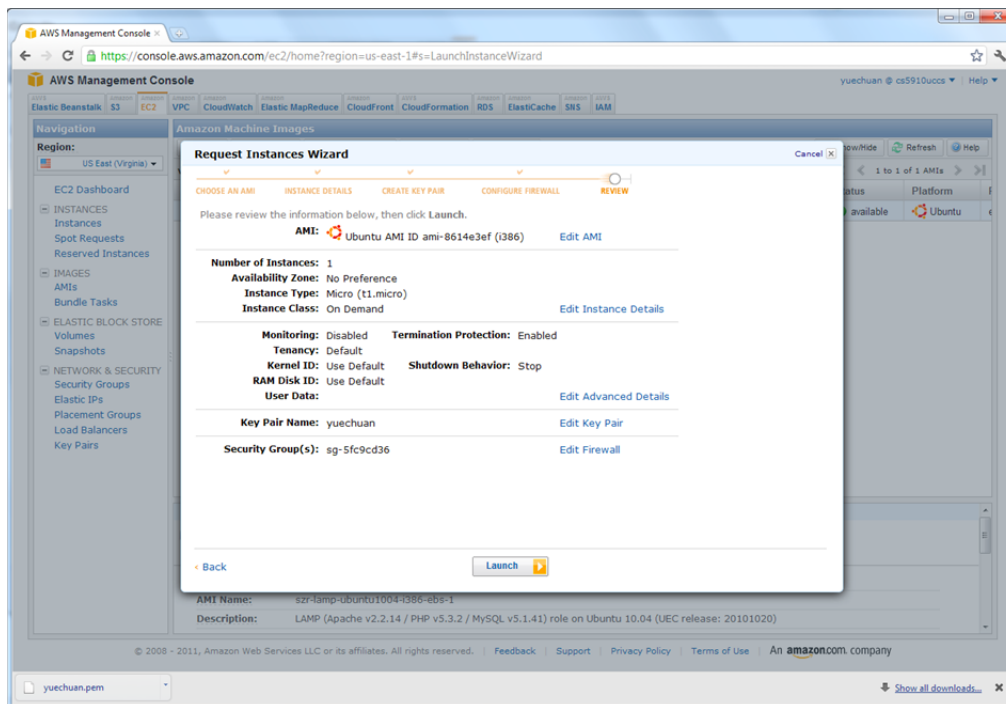


Figure 2. Reviewing the configuration of an EC2 instance before launching it

All the EC2 instances of our class are viewable by the instructor, teaching assistant, and students from the AWS Management Console as shown in Figure 3 (with student names and IDs grayed out for privacy reasons). We think this capability is helpful because students can be aware of each other's instance status just like in a physical lab environment. An EC2 instance may be "stopped" or "terminated" via Web service API or AWS Management Console. When an EC2 instance is "stopped", its configuration and the software installed by a student will be properly saved. A stopped EC2 instance is still listed as one of the "My Instances" in the AWS Management Console (as shown in Figure 3) while its status is shown as "stopped". Later on,

the student can conveniently start the same instance to continue working on the tasks in the same lab exercise or next lab exercise.

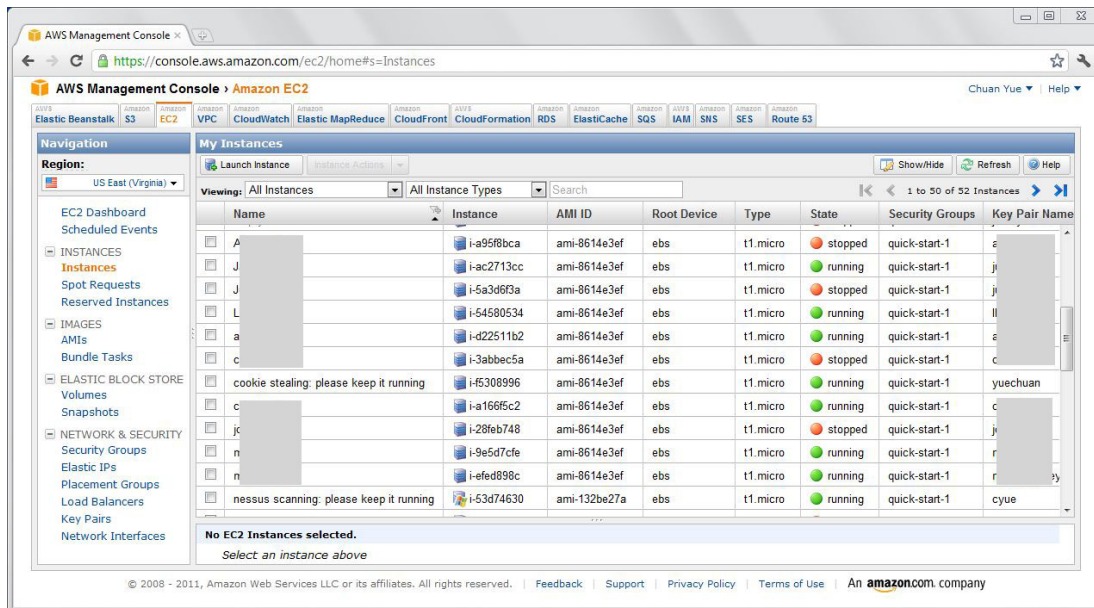


Figure 3. Viewing all the EC2 instances of our class from the AWS Management Console

If an EC2 instance is “Terminated”, it is completely deleted from the Amazon EC2 cloud and is removed from the list of “My Instances”. Therefore, we took several measures to protect students’ EC2 instances from being accidentally terminated by any user. First of all, as shown in Figure 1, we did not give student users the permission to terminate any EC2 instance via either Web service API or AWS Management Console. Second, we advised students to enable termination protection and choose “Stop” as shutdown behavior when they configure their EC2 instances. If the termination protection of an EC2 instance is enabled, even an administrator, i.e. the instructor or teaching assistant, will not be able to terminate this EC2 instance unless the administrator manually disables the termination protection of this instance. Having “Stop” as the shutdown behavior, the EC2 instance will be stopped instead of being terminated when it is shut down by a user. During the whole semester, no EC2 instance in our class was accidentally terminated by any user.

We mentioned that in our practice, we used the instructor’s central AWS account and the IAM<sup>[7]</sup> Web service to create and manage student user accounts. Using this approach, although we configured (as shown in Figure 1) that a student user does not have the permission to terminate any EC2 instance, he or she can still stop or start any EC2 instance in the list of “My Instances” (Figure 3). This is because the “ec2:StartInstances” and “ec2:StopInstances” permissions (Figure 1) do not further differentiate the creators of those EC2 instances associated to the instructor’s central AWS account. We hope Amazon can support a fine-grained access control permission in the future to prevent a user from stopping or starting the EC2 instances created by other users under the same central AWS account. To address this limitation of the current EC2 environment, we asked students not to stop or start EC2 instances of other users. During the

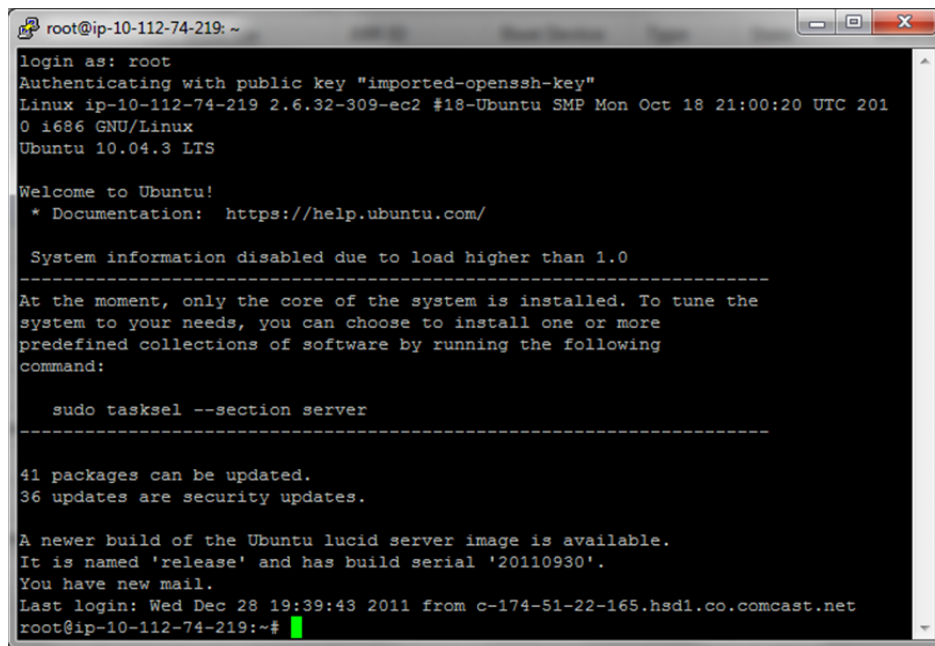


whole semester, our students followed this rule very well, and no accidental stopping or starting of any EC2 instance was reported to us.

To connect to an EC2 instance (at step 6), a student user needs to have the key pair generated when configuring the EC2 instance (at step 3). Hence, technically speaking, a student user can connect to only his or her own EC2 instance. Following the instruction provided by AWS Management Console, a student user may open an SSH terminal and connect to his or her EC2 instance as the *root* user from the SSH terminal. An example of the SSH command is as follows:

```
ssh -i mykeypair.pem root@ec2-10-112-74-219.compute-1.amazonaws.com
```

Here, “ec2-10-112-74-219.compute-1.amazonaws.com” is the public DNS name of this EC2 instance, and mykeypair.pem is a file containing the RSA private key and should be securely stored by a user. As shown in Figure 4, if the SSH connection is successful, a student can work on the EC2 instance as the *root* user just like working on a local Linux machine via a terminal.



```
root@ip-10-112-74-219: ~  
login as: root  
Authenticating with public key "imported-openssh-key"  
Linux ip-10-112-74-219 2.6.32-309-ec2 #18-Ubuntu SMP Mon Oct 18 21:00:20 UTC 201  
0 i686 GNU/Linux  
Ubuntu 10.04.3 LTS  
  
Welcome to Ubuntu!  
* Documentation: https://help.ubuntu.com/  
  
System information disabled due to load higher than 1.0  
-----  
At the moment, only the core of the system is installed. To tune the  
system to your needs, you can choose to install one or more  
predefined collections of software by running the following  
command:  
  
    sudo tasksel --section server  
-----  
  
41 packages can be updated.  
36 updates are security updates.  
  
A newer build of the Ubuntu lucid server image is available.  
It is named 'release' and has build serial '20110930'.  
You have new mail.  
Last login: Wed Dec 28 19:39:43 2011 from c-174-51-22-165.hsd1.co.comcast.net  
root@ip-10-112-74-219:~#
```

Figure 4. Working on lab tasks from an SSH terminal connecting to an EC2 instance

### 3. Design of the Lab Exercises

In this section, we briefly present the contents of the four lab exercises designed for our computer and network security course. We also briefly talk about the ethical considerations in both designing and performing security lab exercises. As mentioned in the above two sections, each student uses his or her EC2 instance as the platform to perform the tasks in each lab exercise independently outside the class hours. After finishing those tasks, each student needs to submit a lab report to answer the questions related to the individual tasks. The link to the complete lab manuals designed by the instructor can be accessed at<sup>[33]</sup>.

### 3.1 Lab exercise 1 – Snort Network Intrusion Detection System (Snort NIDS)

In this lab exercise, students learn Snort<sup>[10,11]</sup> architecture and Snort alerts. Snort is a free and open source network intrusion detection system (NIDS). Students are asked to identify specific attacks by analyzing a packet capture file provided by us. Students are also asked to create custom alerts and identify incoming attacks. Since this is the first lab exercise of this course, each student needs to configure and launch his or her EC2 instance using the AMI named *ami-8614e3ef*. Each student connects to an EC2 instance via an SSH terminal and performs the following tasks:

- Get familiar with this Linux-based EC 2 instance
- Update the operating system and software on the EC2 instance
- Install Snort on the EC2 instance
- Use Snort to analyze a special packet capture file
- Create custom Snort rules to detect the access of certain webpages hosted by the Apache Web server on the EC2 instance

To work on any one of the following three lab exercises, a student can simply reuse this EC2 instance created in Lab exercise 1.

### 3.2 Lab exercise 2 – Linux Firewall

In this lab exercise, students learn how to create Netfilter<sup>[12]</sup> rules using the iptables<sup>[13]</sup> command line program. Netfilter is a Linux firewall. It intercepts and manipulates network packets within the Linux kernel. Netfilter is invoked at the moment of receiving a network packet from a network interface or sending a network packet to a network interface. Netfilter maintains tables containing firewall rules, and it invokes the registered program to handle packets according to firewall rules. Using an EC2 instance, a student performs the following tasks:

- Get familiar with the Netfilter Linux firewall and the iptables command line program
- List the current Netfilter rules defined in the default firewall table
- Send ICMP echo requests from a local PC to the EC2 instance, and from the EC2 instance to an external server such as [www.yahoo.com](http://www.yahoo.com)
- Add firewall rules on the EC2 instance to block both incoming and outgoing ICMP echo requests
- Check open TCP/UDP ports on the EC2 instance
- Hide the SSH service from attackers yet still allow the EC2 instance owner to log in
- Suggest and verify a solution to prevent brute force attacks against SSH
- Suggest and verify at least one more firewall solution to improve the security of the EC2 instance

### 3.3 Lab exercise 3 – Web Security

In this lab exercise, students identify two types of popular Web attacks. One type is Command Injection attacks<sup>[14]</sup>, and the other type is Cross Site Scripting (XSS) attacks<sup>[15]</sup>. We provide students with two Web applications containing these vulnerabilities. We created these two Web

applications based on the examples provided in our textbook<sup>[20]</sup>. Using an EC2 instance, each student performs the following tasks:

- Start the Apache 2 Web server and enable the HTTP traffic on the EC2 instance
- Get familiar with the users and groups pre-created on an EC2 instance
- Get familiar with the Apache 2 related users and groups
- Host the first vulnerable Web application on the EC2 instance
- Identify and verify the command injection vulnerability in the first Web application
- Propose a solution to fix the command injection vulnerability in the first Web application
- Host the second vulnerable Web application on the EC2 instance
- Perform a stored XSS attack against the second Web application
- Make the stored XSS attack more stealthy
- Perform a persistent XSS attack against the second Web application

### **3.4 Lab exercise 4 – Software Vulnerability Exploitation**

In this lab exercise, students learn about the Nessus<sup>[16]</sup> vulnerability scanner, which is one of the most popular vulnerability scanners in the world. Nessus is free for personal use in academics. Students use it to identify system and software vulnerabilities on both Linux and Windows platforms. Using an EC2 instance, each student performs the following tasks:

- Read the Nessus user guide<sup>[17]</sup> to get familiar with the basic concepts, terms, and the usage of this tool
- Install the Nessus 4.4 package on the student's EC2 instance
- Use Nessus to externally scan a Windows EC2 instance configured and launched by the instructor. In this task, the student does not provide the login credential (username and password) of the Windows EC2 instances to the Nessus installed on his or her EC2 instance.
- Use Nessus to externally scan the same Windows EC2 instance configured and launched by the instructor. In this task, the student provides the login credential (username and password) of the Windows EC2 instance to the Nessus installed on his or her EC2 instance.
- Use Nessus to internally scan the student's own Linux EC2 instance
- View and analyze the results of all the above scanning tasks

### **3.5 Ethical Considerations in Designing and Performing Security Lab Exercises**

We emphasize that ethical considerations should be integrated into both the designing and performing of security lab exercises. In addition to considering the general code of ethics and standards of conduct provided by ACM and IEEE etc. <sup>[28, 29, 30, 31]</sup>, we also consider AWS security policies<sup>[6]</sup> and institutional security policies and procedures<sup>[32]</sup>. In our lab exercises design, the vulnerable operating system is only hosted on the instructor's own EC2 instance (e.g., the vulnerable Windows EC2 used in Lab exercise 4); meanwhile, vulnerable applications (e.g., the two vulnerable Web applications) are only temporarily hosted on students' EC2 instances for educational purpose. We asked students to self-study the "Legal and Ethical Aspects" chapter of

our textbook<sup>[20]</sup>, to follow institutional security policies and related procedures<sup>[32]</sup>, not to perform any unauthorized activities, not to attack any other AWS services or other people's EC2 instances, and not to use the learned attacking skills to harm others. The UCCS IT Security Principal Mr. Greg Williams (one co-author of this paper) also emphasized these ethical considerations in one invited talk to our students before performing Lab exercise 1. We would like to remind other educators to also emphasize these and other related ethical considerations in their security lab exercises.

#### 4. Survey Results and Analysis

We designed a survey to obtain insight on students' perception of using Amazon EC2 for hands-on computer and network security lab exercises. The survey consists of 10 questions as shown in Table 1. We asked students to answer this same survey after performing each lab exercise. In addition, from an extra question asked in the survey for Lab exercise 1, we know that only one of the 28 students has taken a course in which Amazon EC2 or other Amazon Web services were used.

We classify the questions in our survey into four categories as shown in Table 1. The first three categories contain eight closed-ended questions regarding students' self-rated skills on Amazon EC2 and Linux (Q1 and Q2), difficulty of the tasks (Q3 and Q4), and the use of Amazon EC2 instances (Q5, Q6, Q7, Q8), respectively. The last category contains two open-ended questions Q9 and Q10.

Table 1. Closed-ended and open-ended questions used in the survey

Category	ID	Question Content
Self-rated skills on EC2 and Linux	Q1	Please rate your current Linux skills: <u>Clueless</u> <u>Beginner</u> <u>Intermediate</u> <u>Advanced</u> <u>Total Guru</u>
	Q2	Please rate your current Amazon EC2 skills: <u>Clueless</u> <u>Beginner</u> <u>Intermediate</u> <u>Advanced</u> <u>Total Guru</u>
Difficulty of the tasks	Q3	The tasks in this Lab exercise are difficult by themselves <u>Strongly disagree</u> <u>Disagree</u> <u>Neither agree nor disagree</u> <u>Agree</u> <u>Strongly Agree</u>
	Q4	How many hours did you spend in finishing the tasks in this lab by using Amazon EC2?
The use of EC2	Q5	Performing the tasks in this lab exercise using Amazon EC2 is more convenient than performing them using my own computer <u>Strongly disagree</u> <u>Disagree</u> <u>Neither agree nor disagree</u> <u>Agree</u> <u>Strongly Agree</u>
	Q6	I would like to use Amazon EC2 in similar security lab exercises in the future <u>Strongly disagree</u> <u>Disagree</u> <u>Neither agree nor disagree</u> <u>Agree</u> <u>Strongly Agree</u>
	Q7	I would like to use Amazon EC2 in other computer science/engineering lab exercises in the future <u>Strongly disagree</u> <u>Disagree</u> <u>Neither agree nor disagree</u> <u>Agree</u> <u>Strongly Agree</u>
	Q8	This Amazon EC2 usage experience is helpful to my career development <u>Strongly disagree</u> <u>Disagree</u> <u>Neither agree nor disagree</u> <u>Agree</u> <u>Strongly Agree</u>
Open-ended questions	Q9	What is the most difficult part in finishing the tasks in this lab by using Amazon EC2 and why?
	Q10	Open comments (please write down whatever comments and suggestions that you have about this lab and Amazon EC2).

## 4.1 Survey Results of Closed-ended Questions

### 4.1.1 Survey Results of Q1 and Q2

In addition to the related computer and network security knowledge, students also need to possess or learn some knowledge and skills on Amazon EC2 and Linux to accomplish the tasks of each lab exercise. Therefore, the two closed-ended questions Q1 and Q2 in the first category ask students to rate their Amazon EC2 and Linux skills, respectively. Students can choose one of the five answer options: clueless, beginner, intermediate, advanced, and total guru.

The survey results of these two questions for each lab exercise are shown in Figure 5. Each column shows the percentage of students choosing each corresponding answer option in each lab exercise. The average skill level in each lab exercise is calculated using Formula (1) and annotated under each cluster of columns in Figure 5.

$$\text{average skill level} = \sum_{i=0}^4 (i \cdot \text{percentage of students self rated as level } i) \quad (1)$$

Here, we converted the five answer options to numeric values where level 0 stands for “clueless”, level 1 stands for “beginner”, level 2 stands for “intermediate”, level 3 stands for “advanced”, and level 4 stands for “total guru”. Strictly speaking, since the responses are ordinal data, they do not necessarily have interval scales. We performed such a conversion simply to ease the comparison of the skill levels from a relative perspective. We can see that these four lab exercises do help student improve their skills of using both EC2 and Linux. The majority of our students ranked their Amazon EC2 skills as clueless or beginner in Lab exercise 1. The average level of Amazon EC2 skills increased dramatically from Lab exercise 1 to Lab exercise 2 and kept increasing to a level of 1.60 in Lab exercise 4. Although not as dramatic as that of the Amazon EC2 skills, the average level of students’ Linux skills also increased from 1.89 to 2.08. We can also see that most of the students have had more or less Linux experience before performing Lab exercise 1.

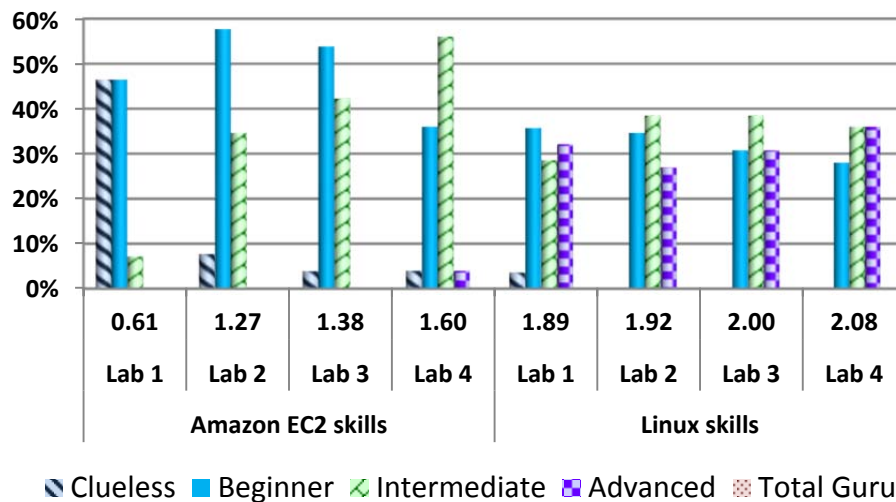


Figure 5. Student self-rating on Amazon EC2 skills and Linux skills

### 4.1.2 Survey Results of Q3 and Q4

Two closed-ended questions Q3 and Q4 are included in the second category as shown in Table 1. Q3 is a five-point Likert scale<sup>[18]</sup> question that asks students to choose one of the five options (“Strongly Disagree”, “Disagree”, “Neither Agree Nor Disagree”, “Agree”, and “Strongly Agree”) in response to a statement. This statement declares that the tasks in a lab exercise are difficult by themselves, i.e., not because of using the EC2 instance. Q4 asks students to report the number of hours they spent in finishing the tasks in a lab exercise by using Amazon EC2.

In Figure 6, each column represents the percentage of students choosing each corresponding answer option in each lab exercise in response to Q3. Figure 7 illustrates the average difficulty level ranked by students on the tasks in each lab exercise and the average number of hours worked on each lab exercise. The average difficulty level is calculated using Formula (2).

$$\text{average difficulty level} = \sum_{i=1}^5 (i \cdot \text{percentage of students choosing level } i) \quad (2)$$

Here, we converted the five answer options to numeric values where level 1 stands for “Strongly Disagree”, level 2 stands for “Disagree”, level 3 stands for “Neither Agree Nor Disagree”, level 4 stands for “Agree”, and level 5 stands for “Strongly Agree”. We can see from Figure 7 that overall, the average number of hours spent by students on each lab exercise agrees very well with the average difficulty level rated by students on the tasks in each lab exercise. Difficulty levels in Lab exercise 1 and Lab exercise 2 are comparable, but fewer hours were spent in finishing Lab exercise 2 than in finishing Lab exercise 1. Considering the learning curves of Amazon EC2 skills and Linux skills illustrated in Figure 5, this inconsistency is reasonable because students spent extra amount of time on learning Amazon EC2 and Linux. The results also indicate that Lab exercise 3 is the most challenging one while Lab exercise 4 is the least challenging one.

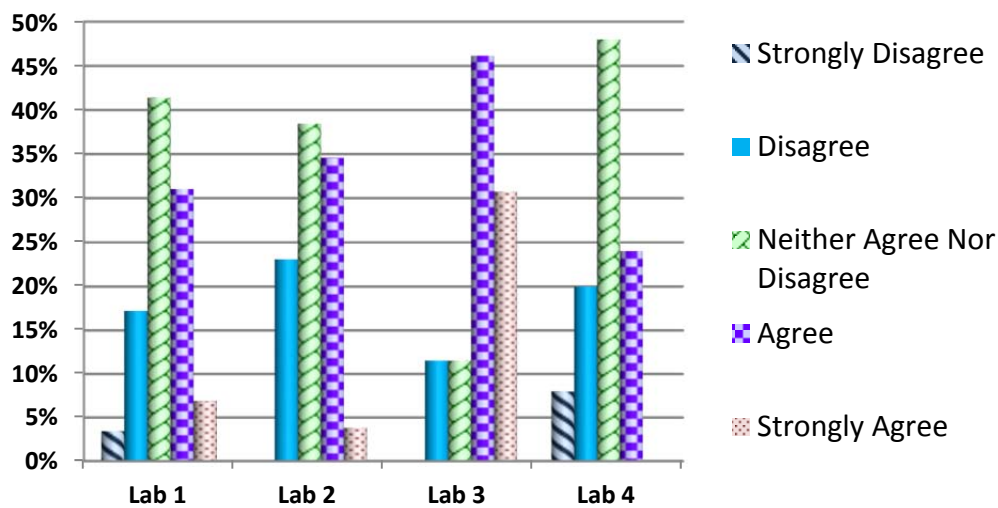


Figure 6. Rating on the statement that the tasks in a lab exercise are difficult by themselves

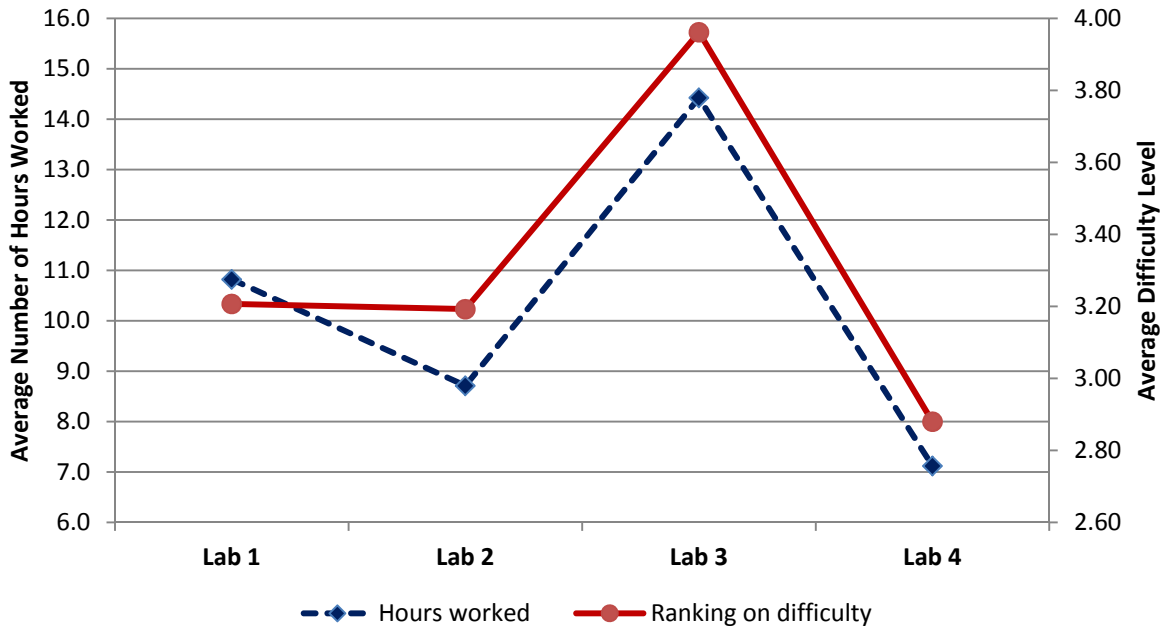


Figure 7. Hours worked and difficulty level on tasks in each lab exercise

#### 4.1.3 Survey Results of Q5, Q6, Q7, and Q8

In the third category, four closed-ended Likert scale questions Q5, Q6, Q7, and Q8 (as shown in Table 1) are given to students to obtain their opinions on using Amazon EC2. Figure 8 illustrates the survey results of these four questions. Each column represents the percentage of students choosing the corresponding answer option in each lab exercise to the corresponding question listed in Table 1. The average level of agreement to the statement in each question is also annotated above the question ID. This average agreement level is calculated using Formula (3).

*average agreement level =*

$$\frac{1}{4} \sum_{j=1}^4 (\sum_{i=1}^5 (i \cdot \text{percentage of students choosing level } i \text{ in Lab } j)) \quad (3)$$

Here, the conversion of the five answer options to numeric values is identical to what we did for Formula (2). We can see that the average levels of agreement to the statements in Q6 and Q8 are very close to the level of “Agree” (with 3.98 for Q6 and 4.02 for Q8). The percentages of students choosing the option of “Agree” and “Strongly Agree” remain the highest and the second highest, respectively, in each lab exercise for the statements in Q6 and Q8, except for the Q8 in Lab exercise 3. There were no or only a few students choosing “Strongly Disagree” or “Disagree”. Therefore, we can conclude that the majority of our students would like to use Amazon EC2 in similar security lab exercises in the future (Q6), and the experience of using Amazon EC2 is helpful to students’ career development (Q8).

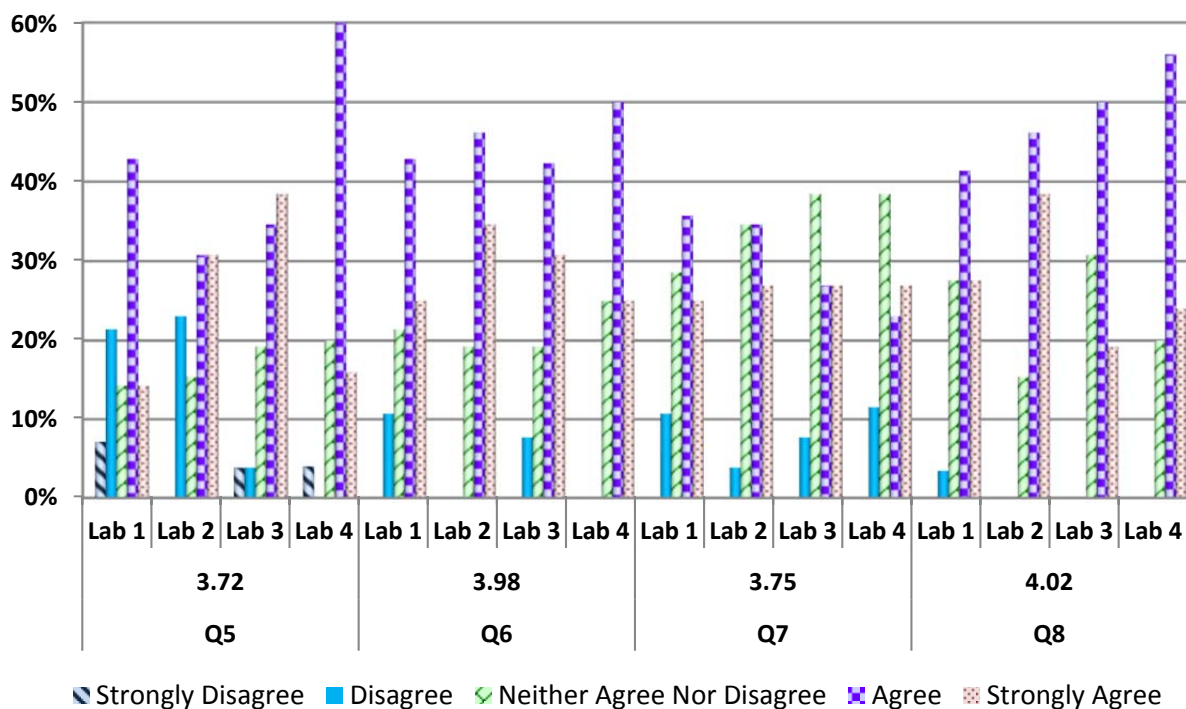


Figure 8. Ranking the statements on using Amazon EC2

Regarding the statement that using Amazon EC2 is more convenient than using a student's own computer (Q5), the average agreement level across four lab exercises is 3.72, which is lower than but somehow close to the level of "Agree". Also, we can clearly see that the levels of agreement in Lab exercises 3 and 4 are obviously higher than those in Lab exercises 1 and 2. In the first two lab exercises, a notable number of students (28.5% in Lab exercise 1 and 23.1% in Lab exercise 2) disagree or strongly disagree with the statement in Q5. However, only 7.6% of the students in Lab exercise 3 and 4.0% of the students in Lab exercise 4 disagree or strongly disagree with the statement in Q5. Meanwhile, the percentage of students who agree or strongly agree with the statement in Q5 is 57.1% in Lab exercise 1, 61.5% in Lab exercise 2, 73.1% in Lab exercise 3, and 76.0% in Lab exercise 4. This percentage keeps increasing from one lab exercise to the next lab exercise. Recalling that students' Amazon EC2 skill level keeps increasing from Lab exercise 1 to Lab exercise 4 as shown in Figure 5; thus, we can conclude that the majority of our students agree or strongly agree that using Amazon EC2 is more convenient than using their own computers once they have learned the basic EC2 skills.

Another interesting observation is that in Lab exercise 1 and Lab exercise 2, the majority of our students agree that they like to use Amazon EC2 in similar security lab exercises in the future (Q6) although fewer students agree that Amazon EC2 is more convenient to use than their own computers (Q5).

Regarding the statement on using Amazon EC2 in other computer science/engineering lab exercises in the future (Q7), the average agreement level is 3.75. The top two options chosen by students are "Neither Agree Nor Disagree" and "Agree" in Lab exercises 1, 2, and 3, and are



“Neither Agree Nor Disagree” and “Strongly Agree” in Lab exercise 4. The agreement level drops to the lowest value 3.65 in Lab exercise 4. Therefore, we can say that some students may have reservations on using Amazon EC2 in other computer science/engineering lab exercises even after they have accumulated experience on using Amazon EC2 in our security lab exercises. We believe that whether using Amazon EC2 in the lab exercises of other courses is beneficial depends on the nature of those courses and the design of their lab exercises.

## 4.2 Survey Results of Open-ended Questions

In our survey, we asked two open-ended questions Q9 and Q10 as shown in Table 1 to allow students to openly comment on the use of Amazon EC2 in their lab exercises. Q9 asks about what is the most difficult part in finishing the tasks in each particular lab by using Amazon EC2. A common opinion indicated by students’ comments across the four lab exercises is that using EC2 does not make a lab exercise itself more difficult. This result is consistent with the results of the closed-ended question Q5. Three representative comments provided by students to Q9 are directly quoted as below:

*“Was not familiar with AWS at all, but it went smoothly after some trial and error.”*

*“I don’t face any problem with AWS EC2 itself. I am happy to learn about AWS EC2.”*

*“Everything was quite easy and fun.”*

There are a few negative comments on Q9, especially in the survey for Lab exercise 1. However, those comments are mainly related to the detailed tasks in a lab exercise instead of the use of Amazon EC2. Three such types of comments on Q9 are directly quoted as below:

*“The most difficult part was dealing with the snort system since it has many options to write a rule.”*

*“I felt that AWS EC2 was easy to use. The biggest part I struggled with is that I have never used SNORT before. I am also pretty weak in Unix.”*

*“Learning iptables was difficult as it took lot of time to study and learn them.”*

The last question Q10 simply asks students to write down whatever comments and suggestions they have about each particular lab exercise and Amazon EC2. Overall, many students indicated that they are in favor of using Amazon EC2 as the platform in all the four lab exercises. They are glad to have an opportunity to learn and use such a leading cloud computing infrastructure. Three representative comments provided by students on Q10 are directly quoted as below:

*“I think that the use of AWS EC2 was a good idea. It allowed me to work from any location but connect to a solid unix operating system. I expect that it will be even more helpful with*

*the research work for this class. Lastly, it gave me valuable training that could be used with an employer and/or startup company, testing ideas, etc.”*

*“I felt this was a great lab. It was challenging and difficult. But, not overbearing. I really enjoyed getting a taste of a cloud computing environment. Cloud Computing is the future. It is fabulous that students get introduced to this concept and actually spend time in the environment.”*

*“I enjoyed using AWS EC2 over the schools VMware vSphere application. With EC2 I was not limited to being on the school network or setting up a VPN just to do my homework. I liked the mobility aspect as a student I could do my lab off the campus network.”*

The third comment is very interesting. The student actually pointed out another advantage of using Amazon EC2 over using the virtual machine environment of a university. To access the virtual machine environment of a university out of the campus, students must first set up a VPN<sup>[19]</sup> connection. Students do not need to perform such an extra step if they use a public cloud service such as Amazon EC2.

In their comments to the question Q10, many students also provided many good suggestions to us. We directly quote three of them as below:

*“It would have been helpful to give a little bit more explanation of how AWS EC2 works either in lecture or in materials give (like a website or a handout). Also give some background on where one would use AWS EC2 and how prevent its usage is. I would also suggest to do a separate lab on AWS EC2 before doing other labs using it.”*

*“I struggled a lot with this lab, but in the process of struggling I learned a lot. I feel that a stronger background in linux would help. Maybe provide some tips on basic linux commands to help the students in the future.”*

*“I see the use of EC2 as both good and bad. Good -- it exposes the student to a cloud environment -- it provides access to a number of different operating environments -- it ensures that each student has the same tools, OS, etc., as the other. There are no unique advantages resulting from hardware, software, etc. -- it provides consistency to the instructor -- they know what's assigned and what the approximate execution limits are. Bad -- it forces the student to work in a character based environment. As a result, they may spend significant time just overcoming the character interface vs. working with the wide range of graphical based tools for the tasks we've done.”*

We will definitely consider these and other suggestions when we revise our lab exercises of this course or design new EC2-based lab exercises for other courses in the future.

## 5. Student Learning and Instructor Evaluation Results

In this section, we briefly present the student learning and instructor evaluation results. The student learning result is very good as shown in Table 2. Overall, the majority of our students successfully completed all the tasks in the four lab exercises. Their scores in Lab exercise 2 and Lab exercise 4 are higher than those in Lab exercise 1 and Lab exercise 3, and this result is consistent with the survey results of Q3 and Q4 presented in Section 4.1.2.

Table 2. Statistics of the scores received by students in the four lab exercises

	Lab exercise 1	Lab exercise 2	Lab exercise 3	Lab exercise 4
Minimum Value	78.0	90.0	50.0	93.0
Maximum Value	100.0	100.0	100.0	100.0
Average	88.59	97.43	85.80	98.65
Median	88.00	98.00	95.00	100.00
Standard Deviation	6.05	2.83	15.03	2.04
Variance	36.61	8.03	225.92	4.15

The instructor evaluation result is also very good. It is the first time for the instructor to teach this course. According to the formal faculty course questionnaire results released by UCCS, the instructor overall rating is 5.1 (out of 6) and the course overall rating is 5.2 (out of 6), which are very good for a large class at UCCS. In addition, many students provided good comments either formally (through faculty course questionnaire) or informally (through email or conversation) to the instructor. For example, they mentioned that “It was a great course”, “We enjoyed the class and found it to be very informative”, “Thanks for a great and rewarding semester”, and so on. As mentioned in Section 1, the four lab exercises are only one component of the course, but we believe they are an essential component for students to actively participate in this course.

## 6. Conclusion

We presented our experience in using Amazon EC2 (Elastic Compute Cloud) as the platform to support four hands-on lab exercises of our computer and network security course. To make our experience valuable for other educators who are interested in using this leading cloud computing service, we introduced the related features and advantages of Amazon EC2, detailed the setup and use of EC2 instances, presented the contents of the four lab exercises designed for our course, and discussed the survey results on students’ perception of using Amazon EC2. The reliability, availability, robustness, accessibility, security, and uniformity of the EC2 environment made the instructor and students prefer Amazon EC2 over physical machines or virtual machines in a departmental computer lab environment. Students were also very excited in learning and using Amazon EC2 in our course, and they felt this Amazon EC2 usage experience is helpful to their career development. The use of Amazon EC2 in this course was funded by an AWS Teaching Grant awarded to the instructor so it is free for us. However, even without the support of this grant, the cost of \$289 for 28 students, one instructor, and one teaching assistant in a semester is not high at all. We conclude that in our case, using Amazon

EC2 is more cost effective than maintaining and supporting a departmental computer lab environment, and we effectively addressed the resource limitation of our existing lab environments and eased the burden on our IT professionals who need to take care of the needs of many courses and maintain the existing infrastructure for college operations. We provide the link<sup>[33]</sup> to our complete lab manuals and instructions. We hope the contents presented in this paper and our detailed lab manuals and instructions can be useful to other educators who plan to use Amazon EC2 in their computer science and engineering courses.

## Acknowledgements

We sincerely thank Amazon for awarding an AWS Teaching Grant to the instructor of this course Dr. Chuan Yue in September 2011. We sincerely thank all the students participated in this course for their cooperation in answering our survey and providing suggestions to us. We also sincerely thank the anonymous reviewers for their valuable comments and suggestions.

## Bibliographic

- [1]. Amazon Web Services, <http://aws.amazon.com/>
- [2]. Amazon Elastic Compute Cloud (Amazon EC2), <http://aws.amazon.com/ec2/>
- [3]. AWS in Education, <http://aws.amazon.com/education/>
- [4]. Amazon Machine Images (AMIs), <http://aws.amazon.com/amis>
- [5]. The Secure Shell (SSH) Protocol Architecture, <http://www.ietf.org/rfc/rfc4251.txt>
- [6]. AWS Security and Compliance Center, <http://aws.amazon.com/security/>
- [7]. AWS Identity and Access Management (IAM), <http://aws.amazon.com/iam/>
- [8]. Amazon EC2 Instance Types, <http://aws.amazon.com/ec2/instance-types/>
- [9]. AWS Management Console, <http://aws.amazon.com/console/>
- [10]. Martin Roesch, "Snort - Lightweight Intrusion Detection for Networks", in Proceedings of the USENIX Conference on System Administration (LISA), pp 229--238, 1999
- [11]. Snort, <http://www.snort.org/>
- [12]. Netfilter, <http://www.netfilter.org/>
- [13]. iptables: The Linux Firewall Administration Program, <http://www.pearsonhighered.com/samplechapter/0672327716.pdf>
- [14]. The Open Web Application Security Project (OWASP) - Command Injection, [https://www.owasp.org/index.php/Command\\_Injection](https://www.owasp.org/index.php/Command_Injection)
- [15]. The Open Web Application Security Project (OWASP) - Cross-site Scripting (XSS), [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [16]. Nessus vulnerability scanner, <http://www.nessus.org/products/nessus>
- [17]. Nessus user guide, [http://static.tenable.com/documentation/nessus\\_4.4\\_user\\_guide.pdf](http://static.tenable.com/documentation/nessus_4.4_user_guide.pdf)
- [18]. Likert scale, [http://en.wikipedia.org/wiki/Likert\\_scale](http://en.wikipedia.org/wiki/Likert_scale)
- [19]. Virtual private network (VPN), [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)
- [20]. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", ISBN: 978-0136004240
- [21]. Marco Balduzzi, Jonnas Zaddach, Davide Balzarotti, Engin Kirda, and Sergio Loureiro, "A Security Analysis of Amazon's Elastic Compute Cloud Service", in Proceedings of the ACM Symposium On Applied Computing (SAC), Security Track, 2012

- [22]. Nicholas Childers, Bryce Boe, Lorenzo Cavallaro, Ludovico Cavedon, Marco Cova, Manuel Egele, and Giovanni Vigna, “Organizing Large Scale Hacking Competitions”, in Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2011
- [23]. Giovanni Vigna, “The 2010 International Capture the Flag Competition”, in IEEE Security and Privacy Magazine, 2011
- [24]. Giovanni Vigna, “Teaching Hands-On Network Security: Testbeds and Live Exercises”, in Journal of Information Warfare, 2003
- [25]. Wenliang Du, “The SEED Project: Providing Hands-on Lab Exercises for Computer Security Education”, in IEEE Security and Privacy Magazine, 2011.
- [26]. Wenliang Du and Ronghua Wang, “SEED: A Suite of Instructional Laboratories for Computer Security Education”, in Journal on Educational Resources in Computing (JERIC), 2008
- [27]. John Hill, Curt Carver, Jeff Humphries, and Udo Pooch, “Using an isolated network laboratory to teach advanced networks and security”, in Proceedings of the SIGCSE Technical Symposium on Computer Science Education, 2001
- [28]. ACM Code of Ethics and Professional Conduct , <http://www.acm.org/about/code-of-ethics>
- [29]. IEEE Code of Ethics, <http://www.ieee.org/about/corporate/governance/p7-8.html>
- [30]. Heinz C. Luegenbiehl, “Themes for an International Code of Engineering Ethics”, in Proceedings of the 2003 ASEE/WFEO International Colloquium
- [31]. Don Gotterbarn, “How the new Software Engineering Code of Ethics affects you”, in IEEE Software, 1999
- [32]. UCCS IT Security, <http://www.uccs.edu/~itsecure/>
- [33]. Our complete lab instructions and manuals, <http://www.cs.uccs.edu/~cyue/teaching/CS5910LabMaterial/>