Backdoor Central: A Cyber Security Education Solution

Ashley Whitson
Jordan Ramos
Mark Wilke

A Proposal Submitted to the Faculty of the School of Information Technology in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Information Technology

University of Cincinnati

College of Education, Criminal Justice, and Human Services

April 2016

	04/25/2016
Ashley Whitson	Date
	04/25/2016
Jordan Ramos	Date
	04/25/2016
Mark Wilke	Date
	04/25/2016
Bo Vykhovanyuk	Date

Table of Contents

Figures

Abstract

Backdoor Central (BDC) is a platform that allows students to access multiple live hackable networks and develop their ethical hacking skills within their courses. BDC is catered toward faculty and students in the School of IT at the University of Cincinnati with a focus on cybersecurity students. The isolated networks simulate real-world exploited machines where the students are able to practice core hacking concepts in a controlled environment. This platform is created using container-based virtualization that allows for a software-based network that is outside of The University of Cincinnati's network. Instructors are also able to customize the base image to allow for further exploration into their course objectives.

Introduction

Cybersecurity is a growing field in the world of Information Technology. With more companies picking up new technology to integrate into their work environment, companies are opening themselves up to attack by unknowingly creating vulnerabilities within their systems. People with the proper knowledge and training to prevent and defend against these attacks are needed now more than ever in this new age of technology.

Backdoor Central aims to offer an educational solution/tool to help prepare the upcoming generations of Cyber Security track focused Students enrolled within The University of Cincinnati. As of right now, the tools and test environments currently being used cost the university thousands of dollars while still not offering fully catered tools/solutions for the education of the students. With Backdoor Central's testing environments created by using container-based virtualization, the students will be able to engage, learn, and hone their skills in a safe and controlled environment.

With this tool, faculty will be able to cater their labs to their syllabus and make changes on the fly to what they believe is pertinent within the Cyber Security field as it continues to grow and change. This gives them the freedom to be more engaging with their class than with the current technologies that are currently in place. Students will be able to gain hands on experience with cybersecurity techniques and get a feel for what it is like handling live systems within real-world scenarios.

Problem

Students in the School of IT at the University of Cincinnati currently do not have a permanent solution to practice penetration hacking skills. Cybersecurity students are expected to have skills in exploiting systems and knowing the best ways to protect them when they enter the professional field. These skills are developed in college by safely hacking into systems that students have full permission and access to through the University of Cincinnati.

The current method to accessing a hackable machine is for students to transfer a virtual machine from their professor to their own external device. One issue with this is that it takes up valuable class time and as the program expands faculty will have to spend multiple classes trying to get the VMs to their students. Another issue is that the VMs can fail over time and students can lose all their work and have to quickly try to get another copy or else they will be unable to do their homework.

Labs are normally faculty created and are very time consuming to set up and there is never a guarantee that the lab will work for everyone. When one student has an issue the professor has to stop the lesson and try to troubleshoot what is going on while the rest of the class waits. Since there is not a standard for lab VMs these problems are reoccurring and frustrating for most students. The time spent trying to get everyone on the same page could be spent delving deeper into hacking and exploring more concepts that students could use in their co-ops or in the real world.

There are paid solutions that exist and they give users access to a live hackable network with lab demos, but they are costly and not a frugal choice for the university. The professors have no way to customize either the environment or the labs. They also don't have any control

over when the system goes down. Students need access to a stable 24/7 environment where they can safely hack and not worry about destroying their VM or why their command is not working on their machine even though it worked for someone else. The solution must be cost effective for the university so all students have access and can practice their skills in some sort of live environment to mimic the real world. Figure one below illustrates a common "off the shelf" product and the different subscription prices per user. The cost of 10 users for a year is $3864. That cost will only increase as the cyber security program expands. This is not a cost effective solution for the university and our solution hopes to cut down on these costs.

Figure 1: ***CTF365 Pricing Table***

Solution

We built UC its own platform that would allow for several isolated networks that are catered towards the learning of students within the Cybersecurity track in the School of Information Technology. These isolated networks would simulate real-world machines that the students could use what they learn in class to breech, infiltrate, and infect in a controlled and safe environment with pre-installed exploits. This is similar to some tools that UC is currently using however the main differences between those and Backdoor Central are that Backdoor Central will be in-house so that the College does not have to spend money on a subscription to a third-party tool, and it will be able to be customized by the instructors to allow for further exploration into their course objectives.

We have explored different options when researching how to accomplish these goals. Chef, Docker, and Puppet were all tools that would allow for the automation and quick deployment of the virtual machines. However it was decided that VMware's ESXI was going to be as the hosting and deployment tool. Instructors would be familiar with the set up and would not have to learn another server/tool extensively in order to use and customize their "labs" with Backdoor Central. Figure 2 illustrates our current network configuration. We first thought to use scripting to do all the work for us, but that proved to be difficult and did not provide a good user experience. After doing some research we found open-source software called noVNC and Guacamole and these were chosen as a better solution to implement our design. As we looked at the two options Guacamole offered more administrative control and it was easier to learn and control than noVNC and it was ultimately the software we chose to implement into our project.

The original plan was to build a webserver and website that would execute scripts to connect to the ESXI cloud. The cloud would then return values back to the front facing webpage in order for a student to use VNC or any other client viewer to access the VMs. Instead we went with the open source software Guacamole that sits on top of a CentOS box that allows users to boot up multiple virtual VMs using their web browser.

A separate website was then created that was hosted on a LAMP configured server which acted as the GUI for students and professors to gain access to Guacamole. This gave them access to the virtual machines hosted on the ESXI server.

The website has four sections separated out by tabs for easy navigation. There is the main home page, which hosts an announcements page as well as a link to the next lab that is due. The next tab brings students to the labs and documentation section. Students can see the current lab due, the past labs that were due and then future labs. Each lab has a small description as well as download links for the lab itself. The next tab hosts the VM creation center. Scripts were created in order to make the dynamic dropdowns work. The dynamic dropdowns has students choose their professor and lab to access the correct VMs they want to use. There was another script that was created to make the “Create a VM” button dynamic based on the values within the dropdowns that were selected. The dynamic button then leads the student to the Guacamole server in a new tab where they log in using credentials given to them by their professor. After logging into Guacamole the student is shown the VM that they selected and they now have full access to do their lab. Lastly, the final tab navigates to a page for professors and admins only. It is password protected and houses all the teacher walkthrough guides as well as hyperlinks to the unlisted guides on Youtube.

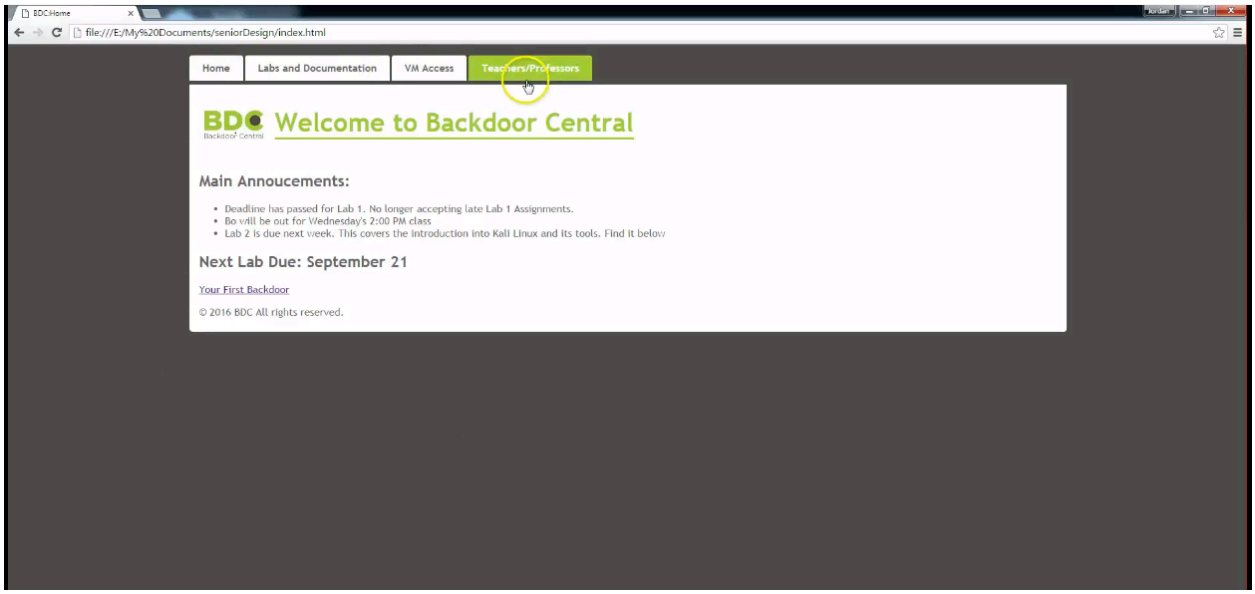

Figure 2: ***Home Page of Website***

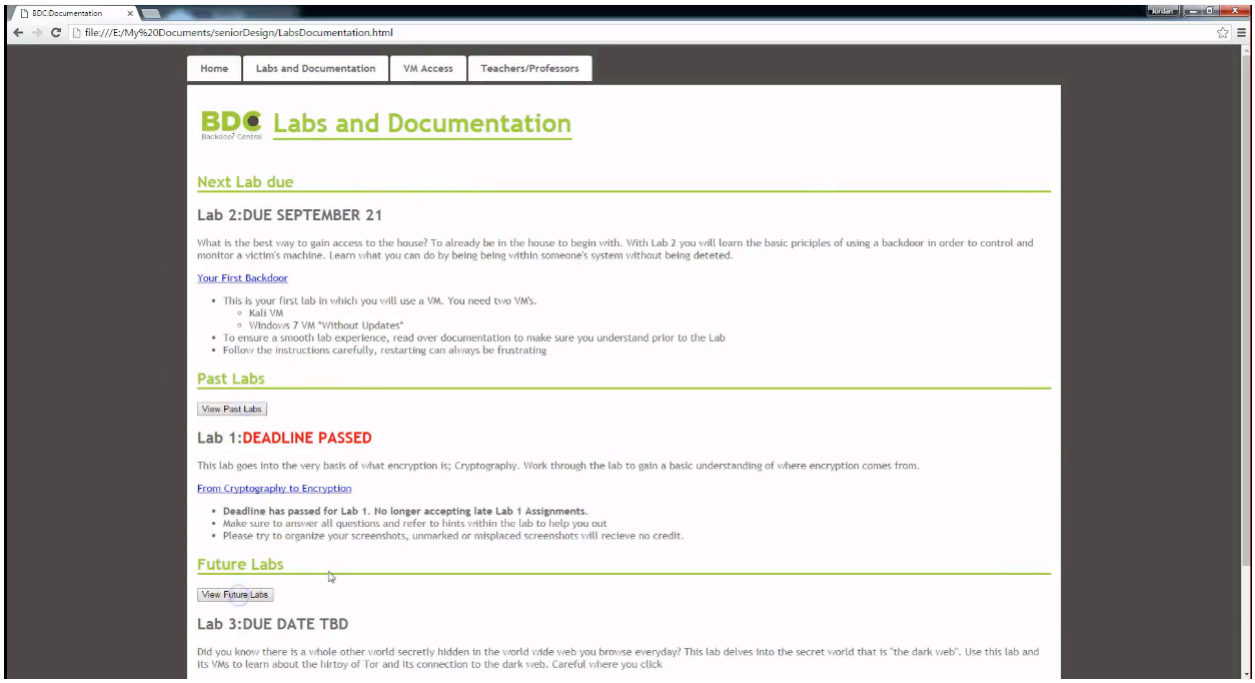

Figure 3: ***Labs Page of Website***

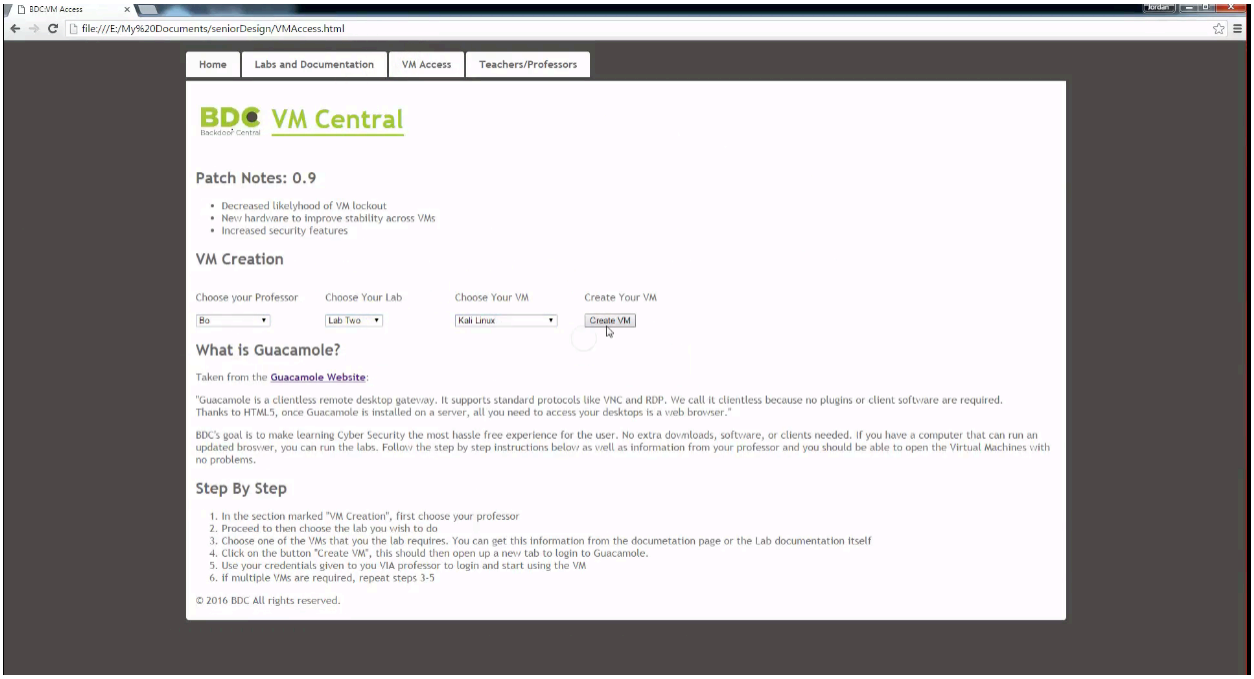

Figure 4: ***VM Access Page of Website***

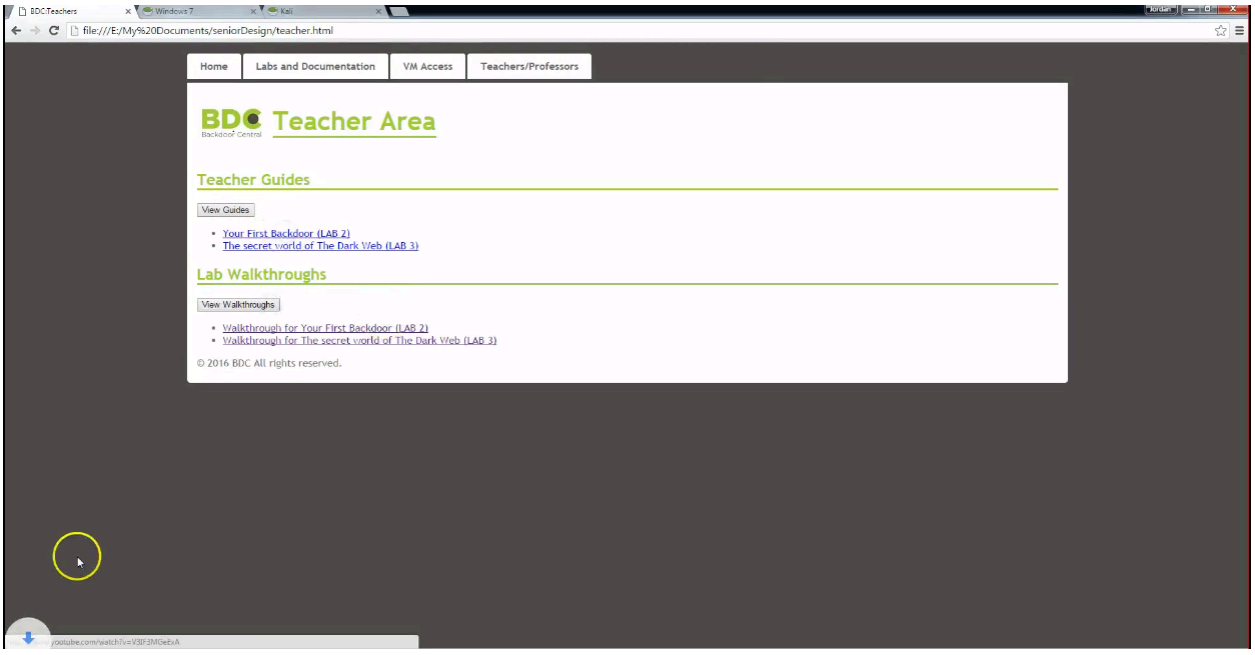

Figure 5: ***Teachers Page of Website***

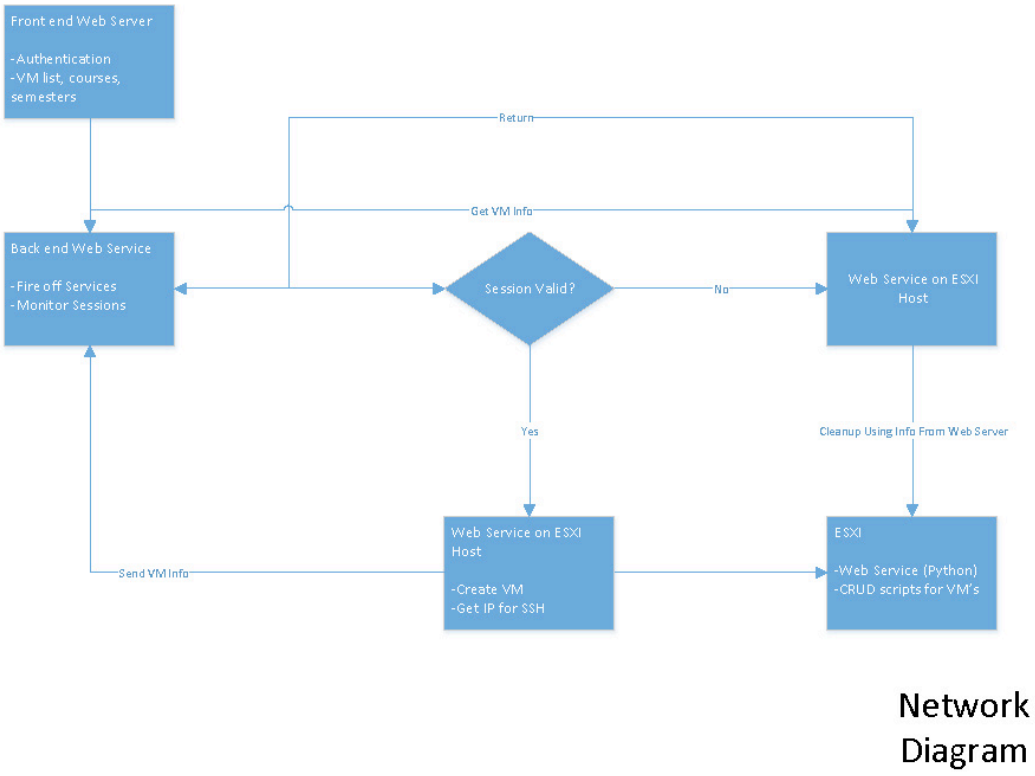

Figure 1: ***Backdoor Central Network Diagram***

User Profile

Students

The student will access the web portal through a standard browser. When they arrive they will be asked to provide a user name and a password. Once they have authenticated they will be able to choose from the classes they are currently enrolled. Each class will have virtual machines

separated by lab and they will be able to choose a class and begin the lab. Once the lab is completed the user will log off and the virtual machine will be returned to its original state.

Faculty

The faculty will access the web portal through a standard browser. When they arrive they will be asked to provide a user name and a password. Once they have authenticated they will be able to choose from the courses they are currently instructing. After a course is selected they are able to make changes to their labs or attempt their labs. They can then save their changes and log off.

Administrators

The admin will run the backend of the system. They will be able to adjust the cloud to add more memory to certain RAM heavy labs or add more virtual machines as needed. They can also make adjustments to the network as required. Like the faculty, the admins will be able to make changes to labs and log into each individual course.

Software and Interface Experience

Students and faculty will use a computer (desktop or laptop depending on preference) with a keyboard or mouse to login and launch the live hackable environment.

Experience with Similar Applications

Students and faculty have had similar experience with accessing virtual machines via the CECH Sandbox. Most, if not all, students will have already taken System Administration and have had extensive use working with VMware and experience with command line terminals. Students may be unfamiliar with hacking or using some of the operating systems, but their classes will help them learn how to use these new technologies.

Task Experience

Since the users are familiar with using virtual machines they would be comfortable with tasks to be completed like logging in or accessing a virtual machine via a website. After a user is logged in they will connect to a course terminal where they can access any remote machine for labs. Cybersecurity courses will cover how to use Metasploit and how to ethically hack remote systems, so students will not need prior experience. A user guide containing all solutions for class labs will be created for faculty or student use.

Frequency of Use:

At least once a week, but hopefully more since we want it to be a main resource for faculty and students. Students are able to access the system outside of class hours to work on their own skills and to experiment with different exploits.

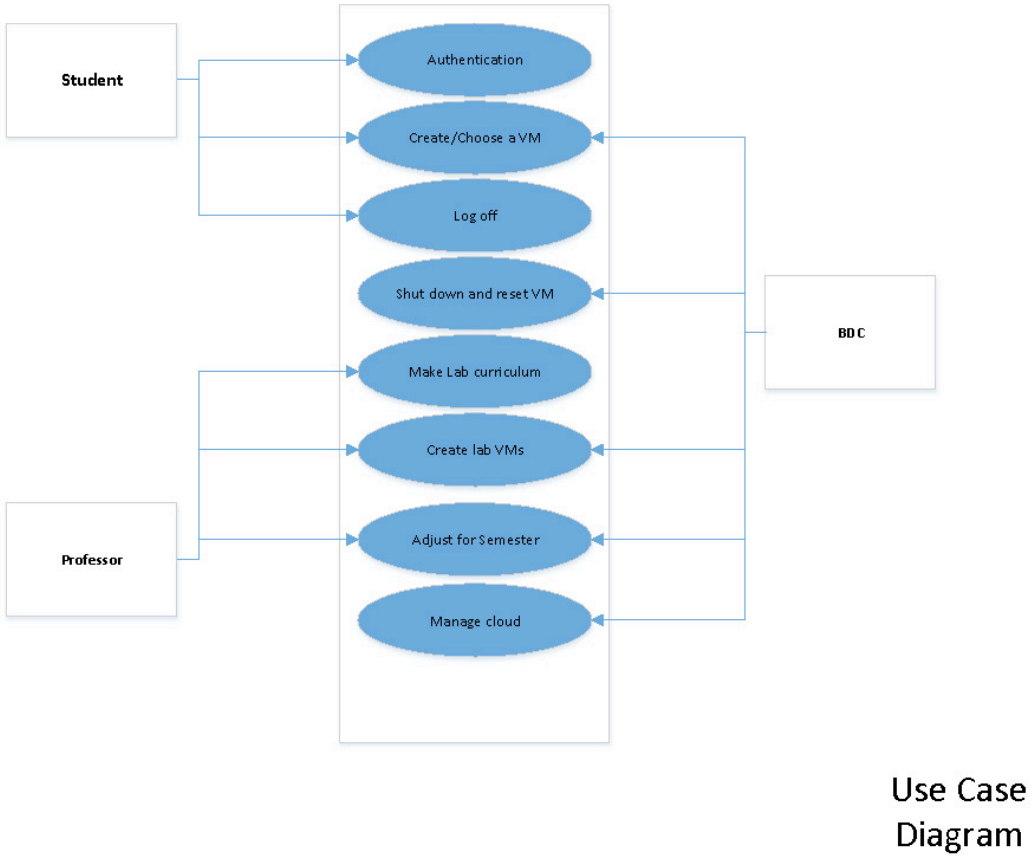

Figure 2: ***Backdoor Central Use Case Diagram***

Timeline

Task Name	Start	End	Duration (days)
Team Contract	9/21/2015	9/29/2015	8
Project Abstract	10/5/2015	10/11/2015	6
User Profile	10/5/2015	10/11/2015	6
Set Up Interviews	10/5/2015	10/8/2015	3
Final Problem Statement	10/12/2015	10/18/2015	6
Progress Report 2	10/19/2015	10/25/2015	6
Use Case Diagram	10/19/2015	10/25/2015	6
Draft Report	10/19/2015	11/1/2015	13
Presentation	11/9/2015	11/15/2015	6
Final Draft Report	11/9/2015	11/29/2015	20
Resources Research	9/21/2015	10/2/2015	11
Acquire Software	10/2/2015	10/7/2015	5
Research Level Design	10/1/2015	10/9/2015	8
Start of Prototype	10/19/2015	11/15/2015	27
Cloud Creation	10/19/2015	11/3/2015	15
Network Creation	10/19/2015	11/3/2015	15
Level Documentation	10/19/2015	11/10/2015	22
Exploitable Machines Creation	10/26/2015	11/15/2015	20
Team Testing	12/14/2015	12/22/2015	8
Student Testing	1/13/2016	1/20/2016	7
Teacher Meeting(s) for Requirements Verification	1/21/2016	1/22/2016	1
Design Poster	3/31/2016	4/7/2016	7
Final Paper	2/15/2016	2/26/2016	11
Practice for Expo	4/8/2016	4/12/2016	4
Acquire Hardware for Expo Demo	3/21/2016	3/25/2016	4

Figure 3: ***Gantt Chart Table***

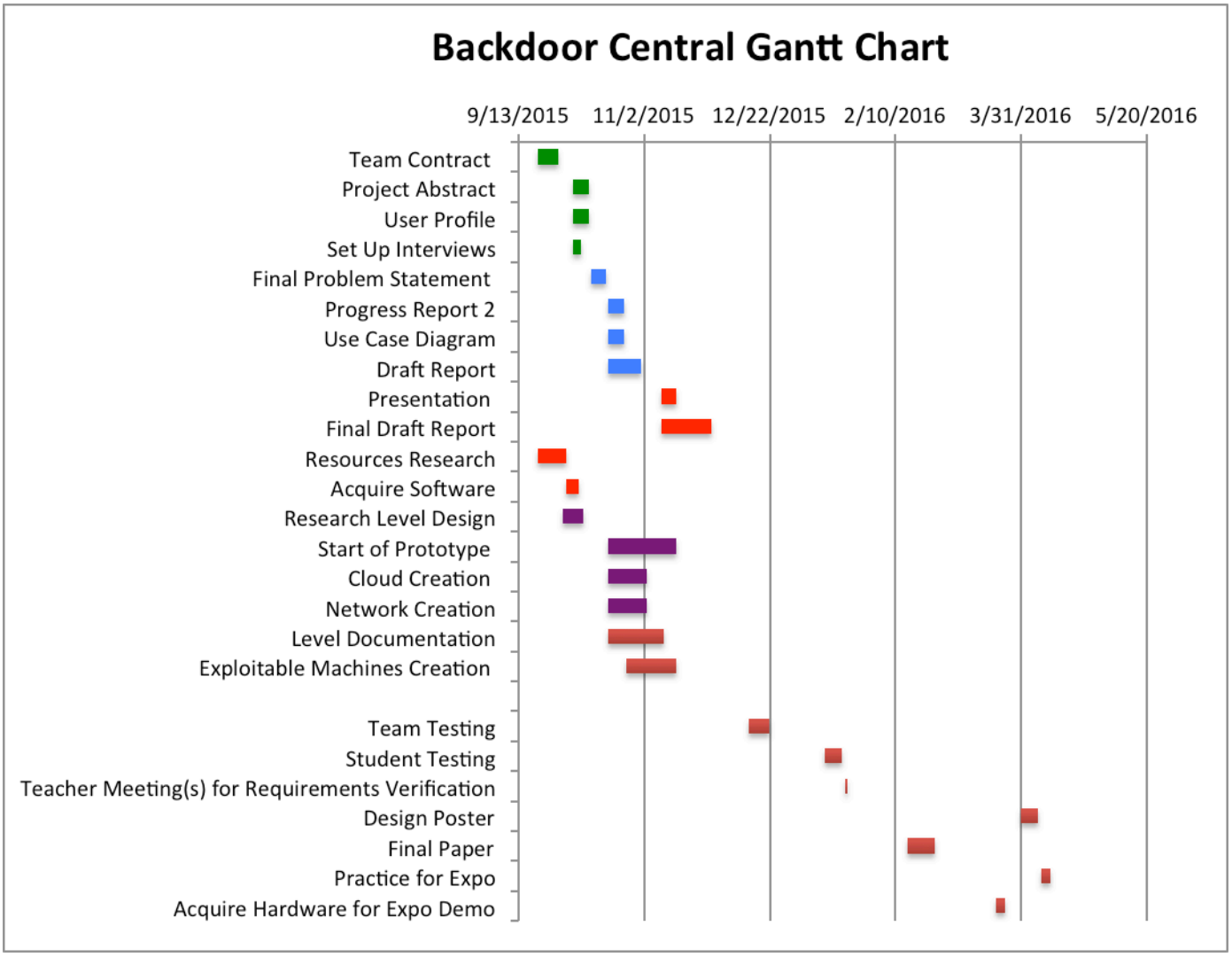

Figure 4: ***Gantt Chart***

Testing

Functional Requirements

1. The web server should allow access to Student, Professor and Admin users.
2. Once logged in, the user should be able to choose the proper class, depending on section.
3. The students should be able to pick virtual machines based on the labs available for the section.
4. The students will have access to proper virtual machines based on their class.
5. Professors should be able to modify existing labs or upload new virtual machines for use.
6. Admins should be able to modify all existing labs and the web interface.
7. Users as well as administrators will be able to log off and end all active sessions.

Non-Functional Requirements

1. The website should have an appropriate color scheme and our logo should be shown.
2. Teaching Guide will be able to explain how to complete each lab.

Test Planning

Functional Requirements

1. The web server should allow access to Student, Professor and Admin users.
   1.a. Username should match the UC Active Directory.
   1.b. Password should be 7 characters long and contain an upper and lower case letter and a special character.
   1.c. No Unauthorized users.
   1.d. A proper error message should be displayed if login fails.
   1.e. The proper menus should be displayed depending on user type.
2. Once logged in, the user should be able to choose the proper class, depending on section.
   2.a. Users will be able to use proper drop down menus to make selections.
   2.b. Students/Professors should only have access to proper section.
   2.c. Admins should have access to all sections.
3. The students should be able to pick virtual machines based on the labs available for the section.
   3.a. Lab selection will change based on how far the class has progressed.
4. The students will have access to proper virtual machines.
   4.a. Students will be able to select which lab they are working on.
   4.b. The proper virtual machine should be displayed based on the requirements of the lab.
   4.c. Students should be able to reset machine if a mistake is made.
5. Professors should be able to modify existing labs or upload new virtual machines for use.
   5.a. Professors will have the option of which labs to show.
   5.b. Professors will be able to upload new virtual machines as needed.
6. Admins should be able to modify all existing labs and web interface.
   6.a. Admins will have access to backend web server.
   6.b. Admins will have all rights that the Professors and Students have.
7. Users will be able to log off and end all active sessions.
   7.a. Log off will end all active sessions and restore them to the starting position.

Non-Functional Requirements

1. The website should have an appropriate color scheme and our logo should be shown.
   1.a. Each page should have the scheme in place and logo in corner.
2. Guide will be able to explain how to do each lab.
   2.a. Guide will have step-by-step directions on how to complete the lab.
   2.b. Guide may have screenshots to help user.
   2.c. User should be able to follow guide with limited technical skill.

Req Number	Item #	Input	Expected Output	actual output	pass/fail	Reasons for Success/Failure	Date
1	1a & 1b	Correct Login	Success Login Screen	Quacamole server lets user in	pass	Quacamole has own user directory	3/21/2016
	1c	Incorrect Login	Incorrect Login Screen	Quacamole server says incorrect login	pass	Quacamole has own user directory	3/21/2016
	1d	Incorrect username	No such Username Exists	Quacamole server says incorrect login	pass	Not what was intended put serves correct purpse	3/21/2016
	1e	Student Login	Student Web Interface	Student only sees what they are given permissions to	pass	Within Website, students only see what professors and admins set up	3/22/2016
	1e	Professor Login	Professor Web Interface	Professor has access to teacher portal and Guacamole server	pass	Professor has access to teacher portal and Guacamole server	3/20/2016
	1e	Admin Login	Admin Web Interface	Admins have all access to Guacamole server and ESXI server	pass	Admins have all access to Guacamole server and ESXI server	3/20/2016
2	2a & 2b	Student Login: Class 1	Class 1 Dropdown Options	Student within class 1 only has proper dropdowns	pass	Students who were only part of certain classes only had certain VMs	3/25/2016
	2a & 2b	Student Login: Class 2	Class 2 Dropdown Options	Student within class 2 only has proper dropdowns	pass	Students who were only part of certain classes only had certain VMs	3/25/2016
	2a & 2b	Professor Login	Edit Dropdowns/choices	Professor has access to HTML to change dropdowns	pass	Professors can edit dropdowns but it might not be intuitive since hard coded	3/25/2016
	2a & 2c	Admin Login	Ability to see and edit all dropdowns	Admin has access to HTML to change dropdowns	pass	Admins have access to edit dropdowns	3/25/2016
3	3a	Professor Login	Ability to hide labs	Professor has ability to hide labs	pass	Professor can hide uploaded labs but it might not be intuitive since hardcoded	3/27/2016
	3a	Student Login	should not see hidden labs	Student can not see hidden labs	pass	Students cannot see hidden labs	3/27/2016
	3a	Admin Login	should see all labs	Admin has ability to hide labs	pass	Admins can hide uploaded labs	3/27/2016
4	4a	Professor Login	ability to take down and upload virtual machines	Professor has ability to add machines to Guacamole Server	pass	Professor can be set as an admin to Guacamole Server	3/29/2016
	4b	Student Login	should not see hidden virtual machines	Student does not have ability to see all machines	pass	Students through use of group policy cannot see certain labs	3/29/2016
	4c	Admin Login	should be able to successfully take down machines and reload new ones	Admin has ability to log into machine via guacamole and terminate connection	pass	Admin has ability to log into machine via guacamole and terminate connection	3/29/2016
5	5a & 5b	Professor Login	Ability to take down and upload virtual machines	Professor cannot add virtual machines to esxi server but can add to Guacamole server	pass	Professors should not have access to the base layer where machines were located was decided	3/29/2016
6	6a &6b	Admin Login	Ability to see all virtual machines and monitor VMs	Admin can log into esxi and Guacamole server to monitor vms	pass	Admin has admin priviledges for Guacamole server and ESXI server	3/29/2016
7	7a	Student Login	Can terminiate active machines	Students can terminate their connects to any machine they start	pass	Students can shutdown or terminate connection to virtual machines they have access to	3/25/2016
	7a	Admin Login	Ability to see active machines and terminate	Admins can kill all connections to active machines	pass	Guacamole offers anims a kill connections buttion	3/25/2016

Figure 6: User Testing Table

Proposed Budget

The proposed budget for this project is approximately $300. We have an in-house server, which will allow us to avoid using any external hosting such as Amazon Web Services. Our major costs will come from upgrading the server to meet our needs. The hope is to not exceed the budget, however if the need arises and no alternatives can be found to overcome obstacles encountered, an increased budget will be discussed among the group members.

For the university to implement our solution they would use the servers they already have. They should only need one or two physical servers based on the enrollment of the cyber track and class needs. These servers would exist on a separate network to ensure the University's network is not prone to a live attack. The university already has licenses for VMWare vSphere client, so there is no associated cost for buying a new software suite. The cost associated with the man-

hours to get the system up and running is not very large. Once our system is set up it requires little maintenance outside of the beginning and end of the semester to prep the images of the pre-built environment.

Asset	Cost	
Dell Power Edge Server	$0	
Upgrades for Server	$300	
Man hours	$340	
Hosting for Server	$0	
Vmware Vsphere 5.0	$0	
	$640	Total

Figure 7: ***Budget***

Conclusion

Cybersecurity is a growing field in the world of Information Technology and it needs properly educated people to fill the open positions. Backdoor Central might not be the final solution when it comes to teaching the students what they need in this field, however it can be a great tool if utilized efficiently. With the ability to be customized, instructors will be able to keep up with technology and what becomes relevant to know within the field. With the level system in place of traditional labs, our goal is for the "labs" to be more engaging and easier for students to see how the knowledge builds on itself.

Developing and implementing Backdoor Central in-house will save the university thousands of dollars a year by not having to pay a subscription fee and instructors will be able to get in-house help and troubleshooting for any problems that they might encounter. The latter will especially be important as the instructors get comfortable with customizing their own machines

for the students to practice on and exploit. Overall, Backdoor Central will be a great tool for both the instructors and the students to utilize and further their growth in the realm of cybersecurity.

References

CTF365, n.d. Web. 20 Sept. 2015

Jumper, Michael. "Guacamole Manual." Guacamole Manual. Glyptodon LLC, 2015. Web. 15 Mar. 2016.

"Metasploit Documentation." *Metasploit Documentation*. Metasploit, n.d. Web. 20 Sept. 2015.

"Official Kali Linux Documentation." *Kali Linux*. Kali, n.d. Web. 20 Sept. 2015

"OWASP WebGoat Project." *OWASP*. OWASP, n.d. Web. 20 Sept. 2015.

Price, Ed. "Hyper-V: Script for Reverting Snapshots VMRevert." *Tech Net*. Microsoft, 30 June 2011. Web. 15 Oct. 2015.

"Restore-VMSnapshot." *Tech*. Microsoft, n.d. Web. 15 Oct. 2015.

Siebert, Eric. "Top 10 PowerShell Scripts That VMware Administrators Should Use", http://www.virtual-strategy.com/2008/12/10/top-10-powershell-scripts-vmware-administrators-should-use *Virtual Strategy*. Virtual Strategy Magazine, 10 Dec. 2008. Web. 15 Oct. 2015.

Uys, Chris. "Find Snapshots and Send Email to User/users." *Vmware Communies*. Vmware, 11 Aug. 2008. Web. 15 Oct. 2015.