Lowering the Barrier to Entry: Open Source Cyber Tools

Instructor Note: The overall intent of this lecture is to introduce the MIDN to the concept of open source tools. Specifically, we will focus on offensive cyber operation (OCO) tools. **A key takeaway for the MIDN should be that the barrier to entry for OCO is low**. That is, there exists freely available platforms, operating systems, programs, and the like (e.g., exploits, vulnerabilities, software) that allow a user to have an impact in cyberspace with little-to-no knowledge of how they (actually) work. It is a point-and-click (cyber) world. MIDN will not be graded for completing this lab. However, they will not be able to complete any other assignments throughout the course without doing so.

Proposed Class Structure:

1. Faculty should watch the below video prior to class. Note, the video is not visible to students. The video demonstrates successful execution of the lab.
2. Review homework and answers from previous class. This is optional.
3. Provide MIDN a brief lecture per the overall intent of the lab, and point them to the SY401 lab on the webpage to begin.
4. **Make explicitly clear that MIDN should shut down their VM when not in use**. At the end of each class. We have many students that require the server resources.
5. Have the MIDN work through issues when they run into problems. Assist Socratically, but don't provide the answer unless you feel it necessary.
6. The lab is due a week from today. What MIDN do not complete in class, they must complete for homework before the next lab.
7. Provide feedback on how to improve the lab.

Overview

Lowering the barrier to entry is an economic phrase used to describe markets. That is, the higher the barrier to entry and exit, the more prone a market tends to be a natural monopoly. The lower the barriers, the more likely the market will become a perfect competition.[1]

In the cyber context, the higher the barrier to entry and exit, the more an individual needs to have a priori knowledge or skills to create or use a tool. For example, if there is a high barrier to entry then an individual may need to understand the C programming language, the UNIX operating system and how to navigate the file structure using only a command shell, and the detailed functionality of the TCP/IP protocol stack. On the other hand, lower barrier to entry means that the less a priori knowledge and skills an individual needs to use a tool. For example, the individual may only need to know where to download the tool (e.g., a URL), how to download the tool (e.g., save-as), how to install the tool (e.g., double-click on the file and follow on screen prompts), and to execute the tool (e.g., navigate the tool functions). In essence, how to operate the tool.

Open Source Tools and Offensive Cyber Operations (OCO)

For SY401, open source 'tools' in the TCP/IP cyber domain context typically refer to the platforms, operating systems, programs, and the like that can be used to enable offensive or defensive cyber operations. Open source tools typically are crowdsourced by a community of volunteers. This means that the development of these tools are decentralized and successfully achieved through collaboration. Examples of more common open source tools include openstack (platform), Ubuntu Linux (operating systems), OpenOffice (program), and nmap (and the like).

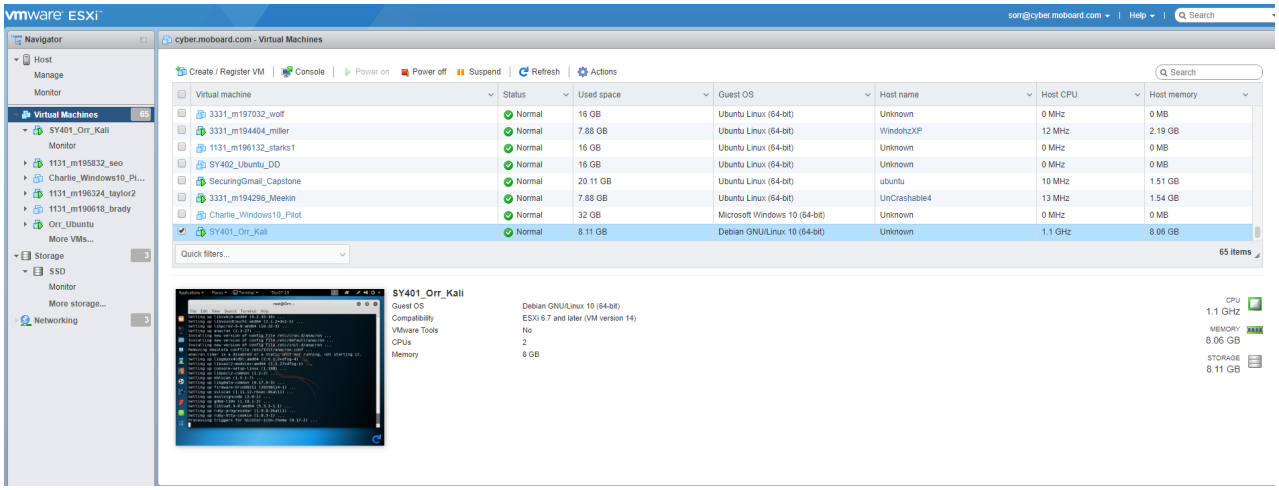
In this class we are going to explore open source tools developed for offensive cyber operations. Per DoD Joint Doctrine (JP3-12), Offensive cyber operations is the term used to describe the use of "*power and force in and through cyberspace*".[2] As you have learned in previous classes, Cyberspace is a domain of war recognized by the Department of Defense. The open source tools we will use to operate in cyberspace include Metasploit (platform), Kali Linux (operating system), Maltego (program), and John the Ripper (and the like).

It is also important that when discussing, learning, or using any of these open source tools; that they are considered in the context of end-to-end operations.

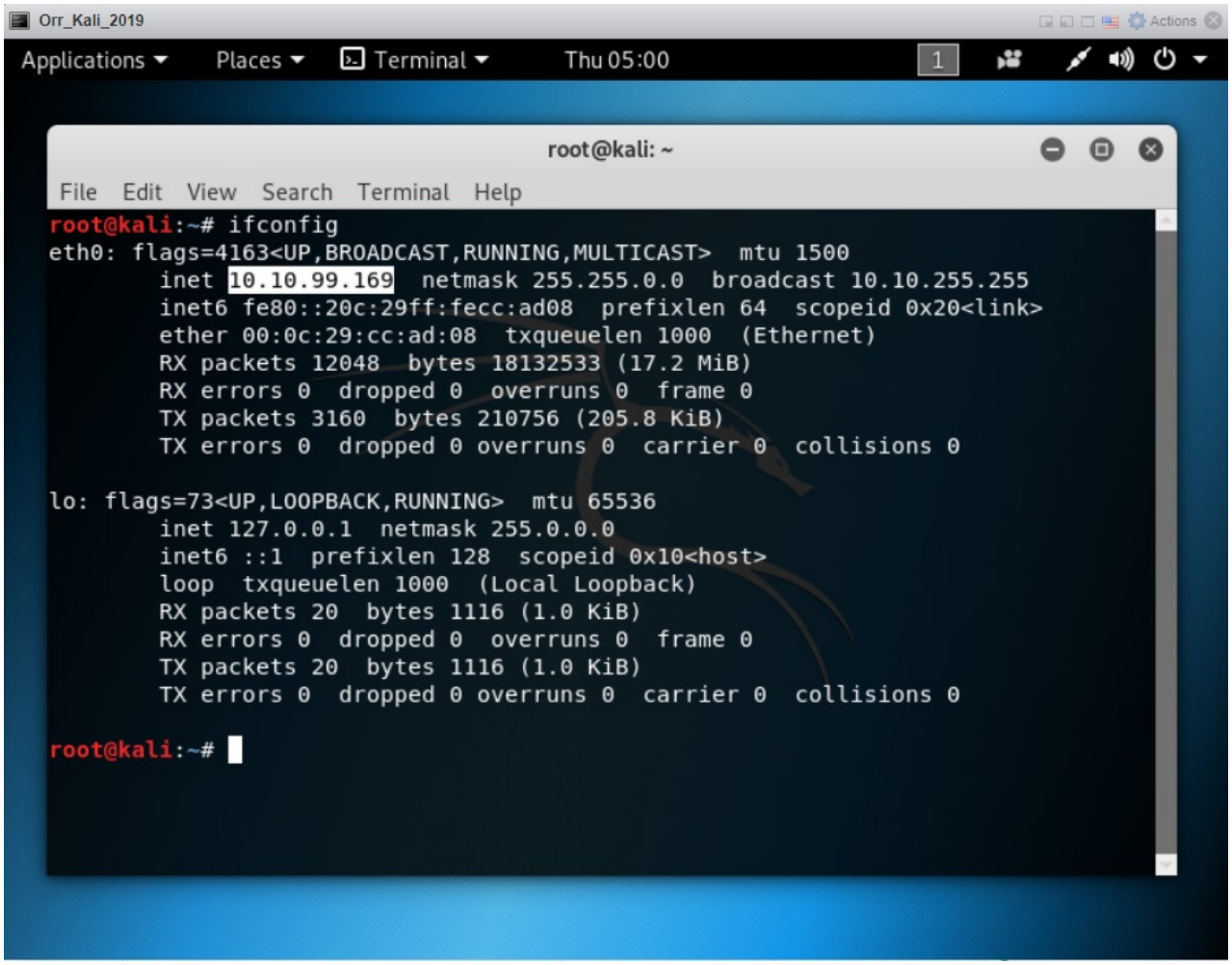
Lab Deliverables

MIDN will submit a **single PDF document** to your Professor that contains two screenshots as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file. Submission of a document other than a PDF will result in an automatic deduction of 5% of the overall grade.

- Cyber.Moboard.Com -> Virtual Machines screenshot of configured VM.



- Kali Linux VM screenshot with IP address displayed in the Terminal.



The subject line of the email should be in the following format:

```
SY401 [Section Number]: [NAME OF LAB] (alpha)
```

For example:

```
SY401 1111: Lowering the Barrier to Entry - Open Source Tools (m123456)
```

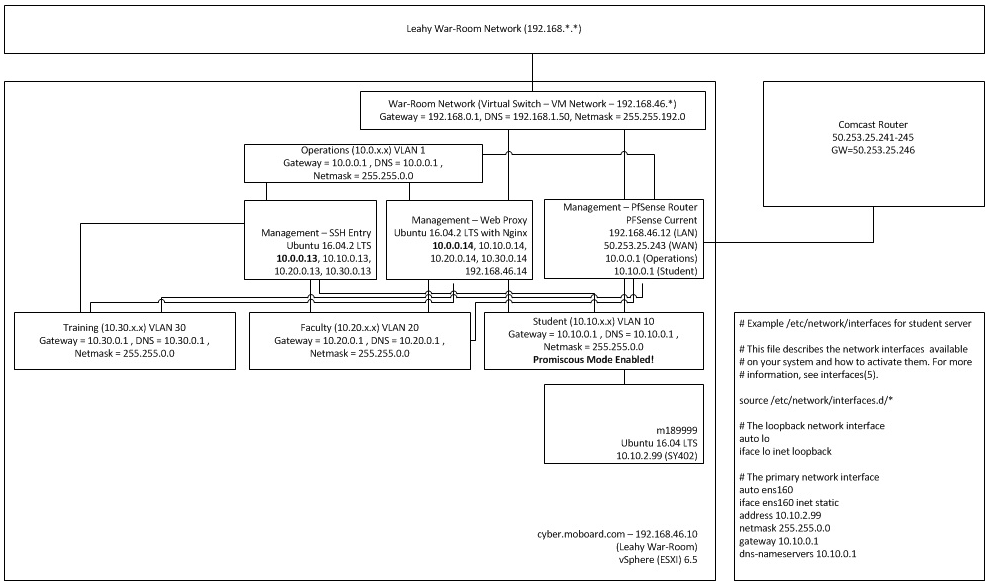
MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Preparing for the Lab

In order to perform this lab you will need to already have a method to SSH into our servers, hopefully you already have Putty installed, if not install it now. You will only need to use the web GUI to connect to the ESXi server for the initial install of your server during the next lab, after that point all connections should be made via the SSH gateway. Using SSH has its advantages, and with this you will be able to connect to your server from anywhere on campus.

Our Virtual Environment

We will be using a server currently located in the Leahy War-Room for the duration of this course. Next week you will each install your own Kali Linux installation.



This server is a **Dell R815** with **256GB of RAM** and **Four 16 Core AMD 6376** Processors, storage consists of a **six 500GB SSD** drives pooled together in a **RAID 5** configuration with 2.3TB of usable space available and a single **Intel 750 400GB PCIe SSD** referred to as datastore and Intel in the system respectively. The infrastructure Virtual Machines are stored and running on Intel storage and all of your student VM's will be running on the larger datastore.

Accessing Our Virtual Machines

The machines that you install will be accessed through a firewall and gateway, all part of the virtualized server. With a flow like:

```
pfsense router (port 22 forwarding) → Ubuntu gateway (port 22) → your virtual server
```

```
pfsense router (port 443 forwarding) → Ubuntu proxy (port 443) → ESXi Web Interface (port 44
```

When you connect to the IP address of the pfsense router on port 22, it will automatically forward you to port 22 on the gateway virtual machine. For the web forwarding it is a bit more complicated, as pfsense forwards ports 443 to the proxy which provides SSL encryption and then creates a new connection to the ESXi host and forwards back the results, in essence the proxy is a **man in the middle**. The proxy has a valid SSL certificate, when you are on the ESXi server, what does it's certificate look like, do you ever see it?

Connecting to the SSH Gateway

- **SSH Address** - cyber.moboard.com
- **Default username** - malpha - example *m201234*
- **Default password** - gonavy123

Immediately change your password, do not use your academy credentials. Feel free to look around the gateway.

Connecting to the ESXI (vSphere)

- **Web Address** - cyber.moboard.com
- **Authenticate to Splash Page**- **Username**: esxi **Password**: See Instructor
- **Web page Default username** - malpha - example *m201234*
- **Web page Default password** - gonavy123

Immediately change your password, do not use your academy credentials. Feel free to look around the ESXi server, as this will help you to understand its capabilities. Your account does not have the access to do any damage, so click through all of the options. **Note:** VMWare does not count an initial capital letter as a capital letter to meet complexity requirements...

Kali Linux Distribution

"If I had eight hours to chop down a tree, I'd spend six hours sharpening my axe." -Abraham Lincoln

Instructor Note: In class we will go through the Kali Linux installation per the instructions below. Make sure that any MIDN not completing the installation in class understands it should be completed before the next class. Otherwise, they will find themselves behind.

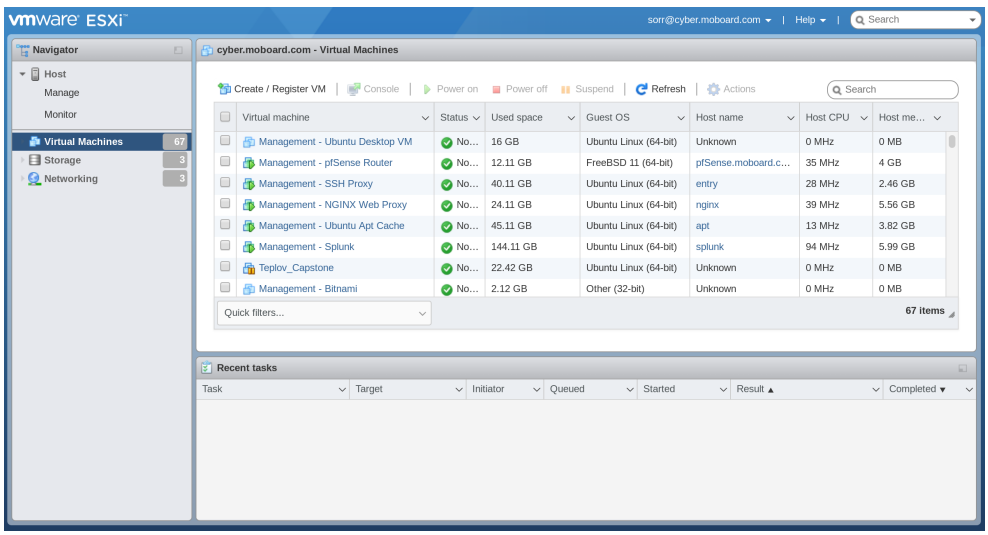
Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services. It is expected that MIDN will become familiar with this operating system by downloading, installing, configuring, updating, and operating it throughout the class. It is important that you maintain your system by keeping a pulse on the available updates, and changes to the operating system and open source tools it includes.

Just as every marine requires a mastery of many different weapons. Every cyber operator requires mastery of many different tools. This class begins the journey of ensuring you have the warfighting capability knowledge of a cyber operator. It is important that you maintain your weapon system through the necessary updates, security patches, enhancements, and the skills and knowledge necessary to operate them. To begin, we will install, configure, update, and become familiar with our cyber operator weapons systems.

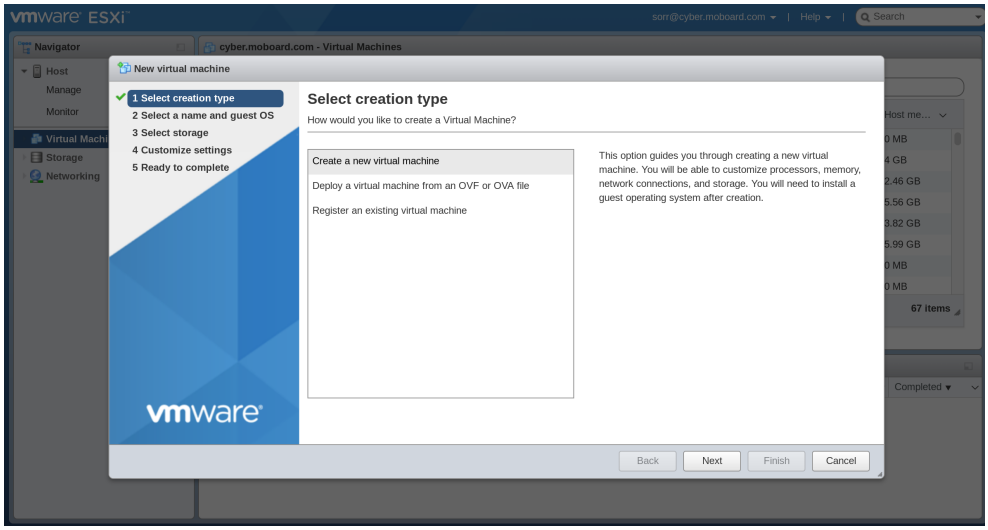
Complete for homework what you do not complete in class.

Instructor Note: As of this writing, the most recent version of Kali Linux is 2019.2.

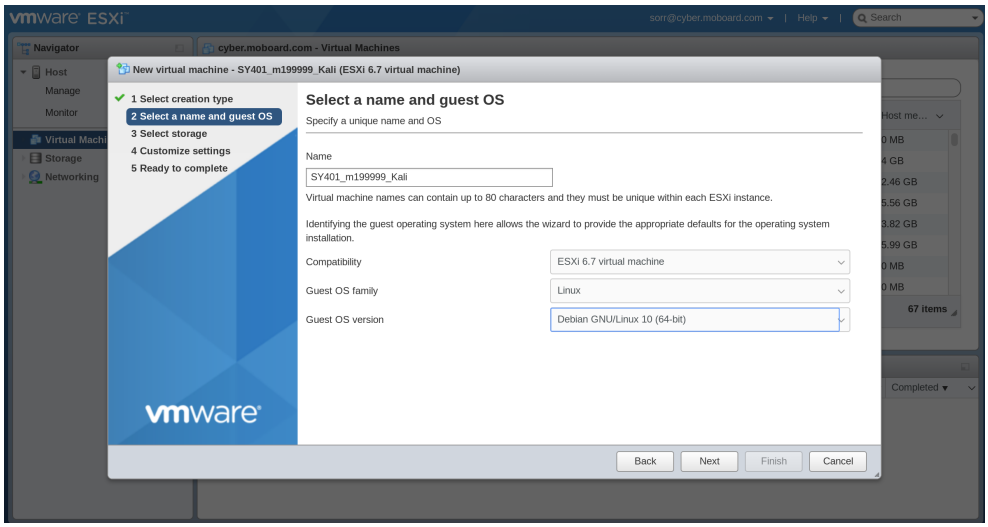
- Install the Kali Linux operating system on your assigned virtual machine. Below are screenshots for each step.
- Create a new Virtual Machine. Select Next.



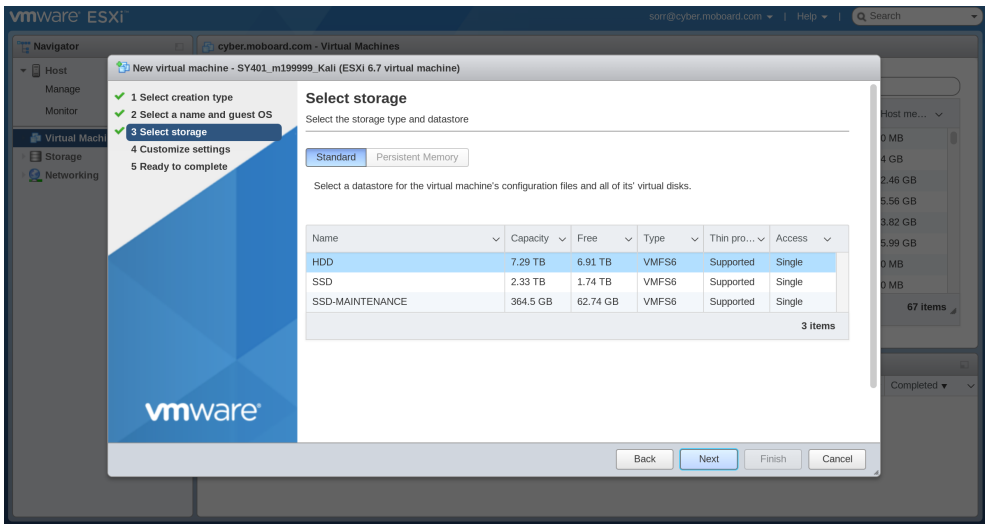
- Create a VM.



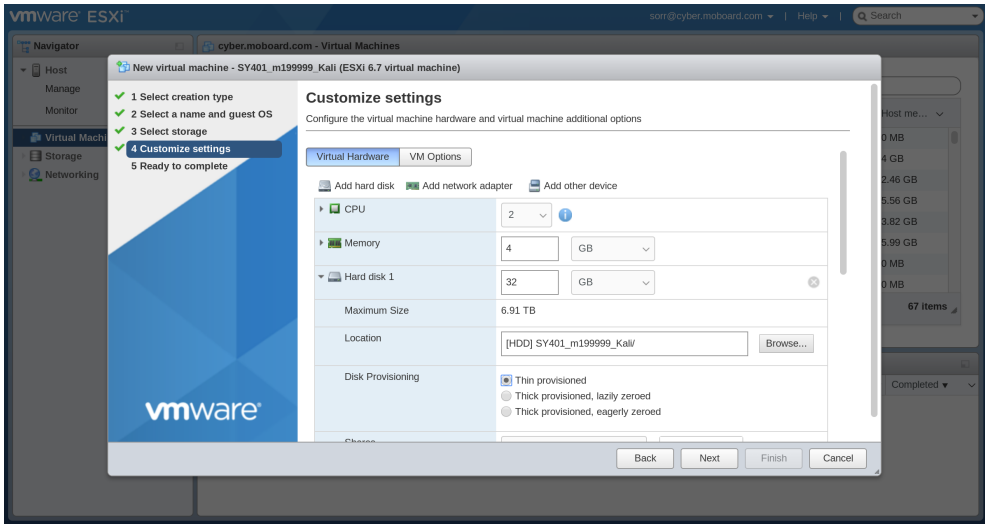
- Name your virtual machine (**SY401_alpha_Kali**). Select Linux as the Guest OS family. Select Debian GNU/Linux 10(64-bit) as the Guest OS version. Select Next.



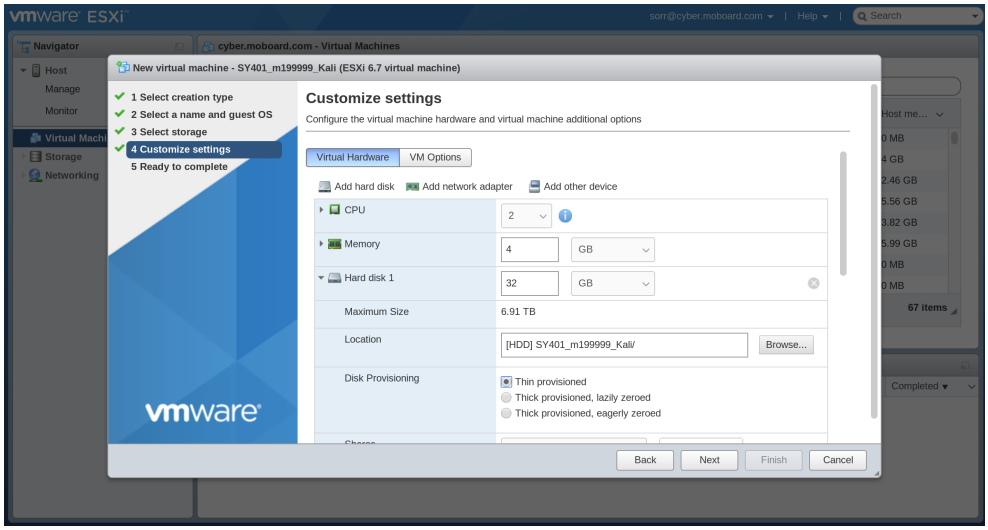
- Select HDD. Select Next.



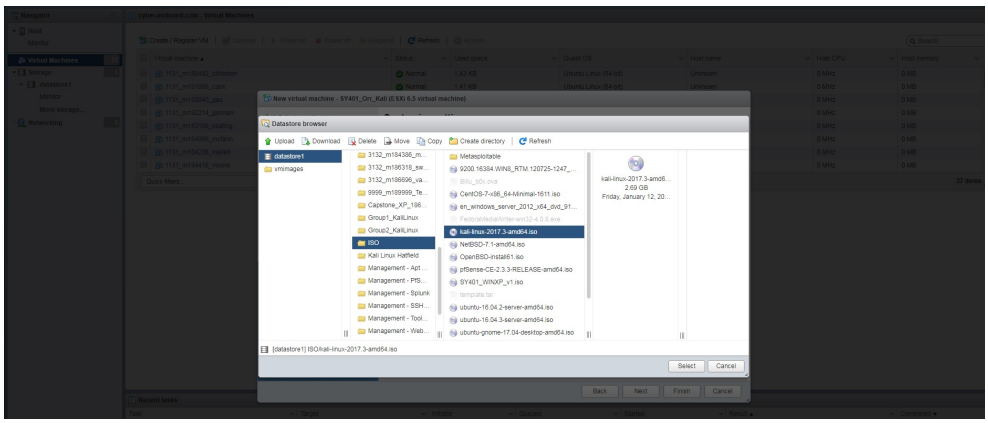
- Change CPU to 2, memory to 4GB, and Hard disk 1 to 64GB. **Change Network Adapter 1 to Student**. Select Browse.



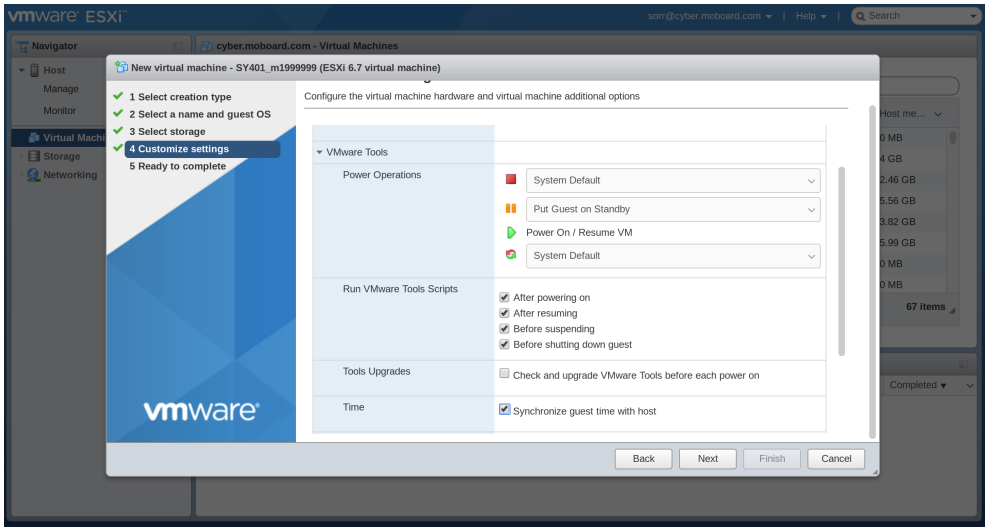
- Select the Hard Disk drop-down arrow. Check the 'Thin Provisioned' option under Disk Provisioning.



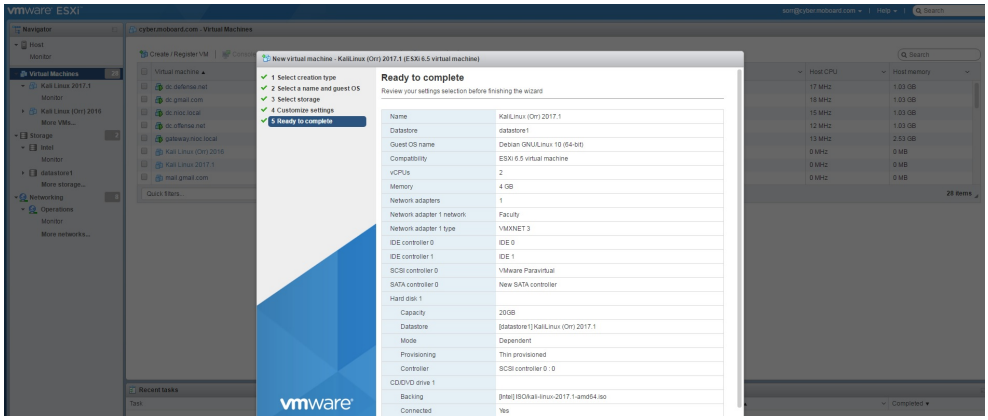
- Under CD/DVD, Navigate to datastore1 -> ISO and select kali-linux-2019.2-amd64.iso



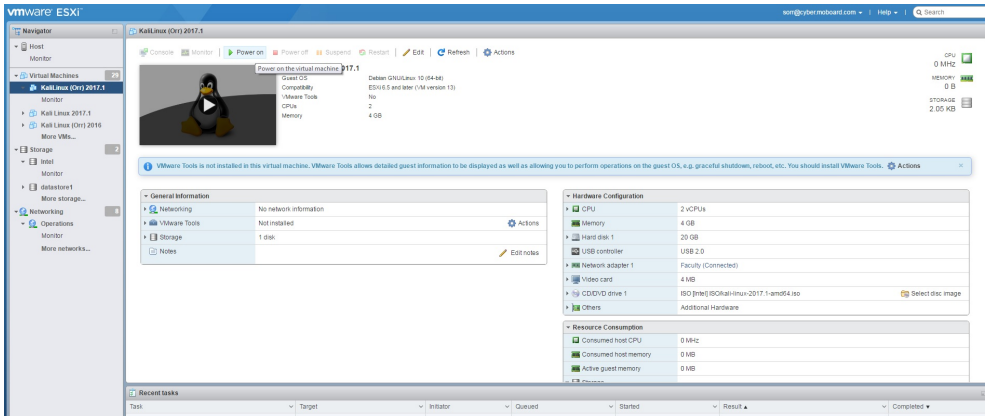
- Select VM Options. VMWare Tools -> Time - Check Synchronize guest time with host.



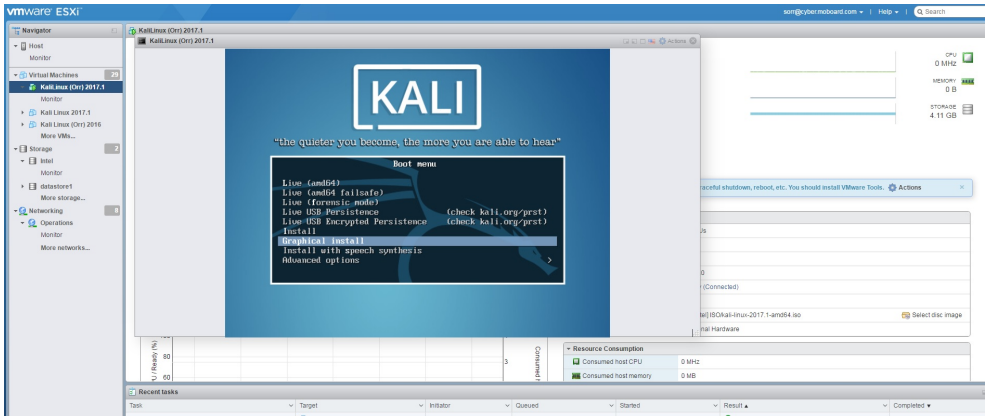
- Review your options and continue with the installation.



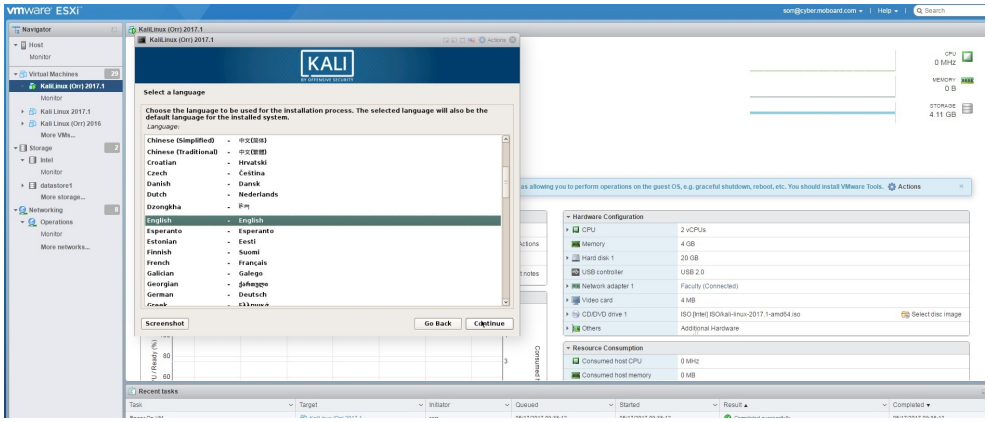
- Power on the VM.



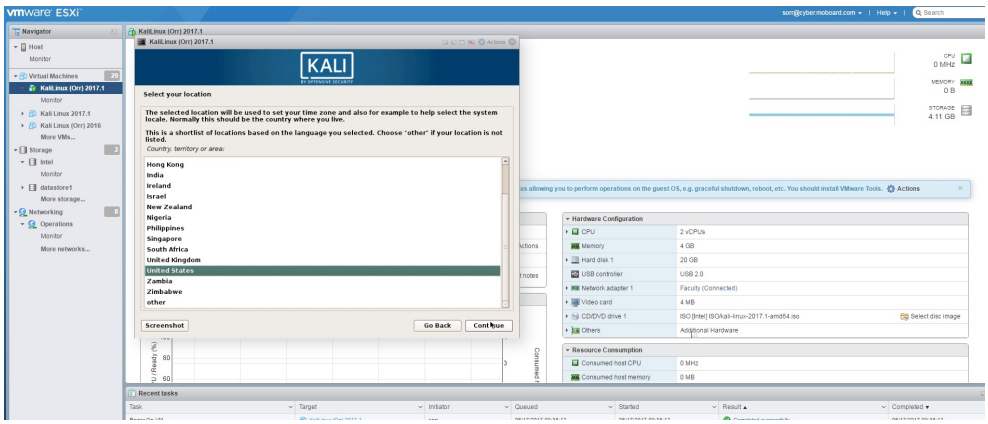
- Select Install or Graphical Install.



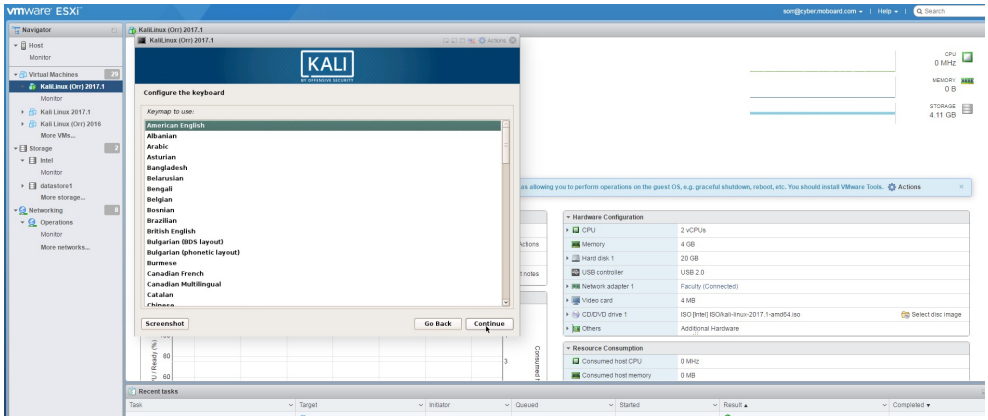
- Select English. Select Continue.



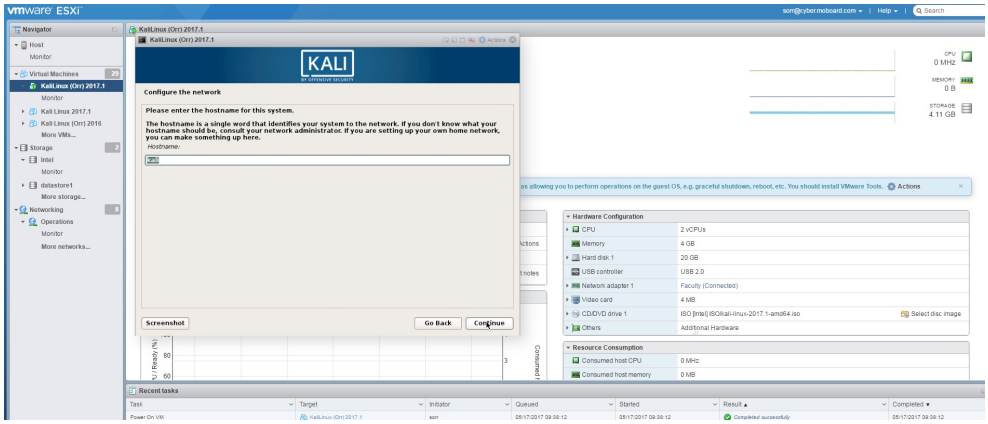
- Select United States. Select Continue.



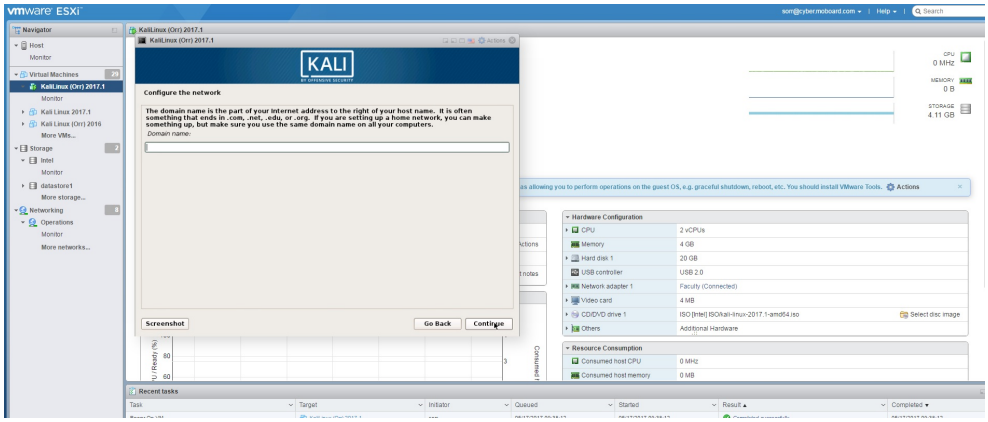
- Select American English. Select Continue.



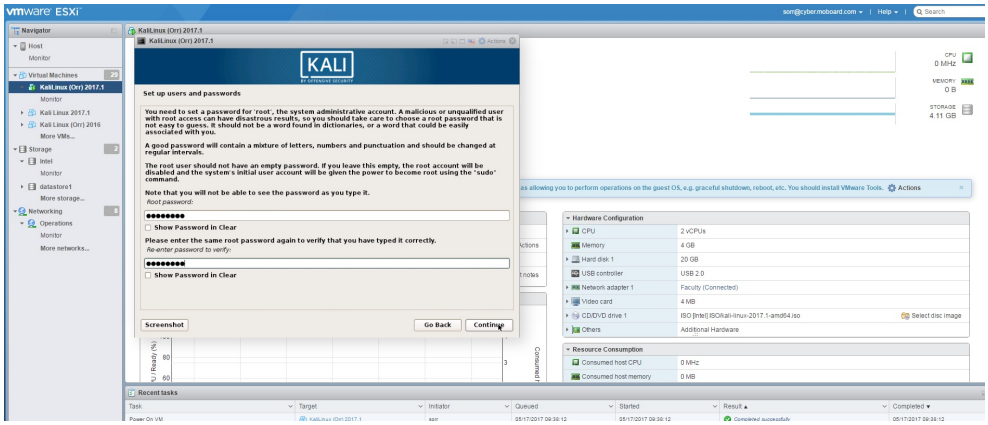
- Select Continue.



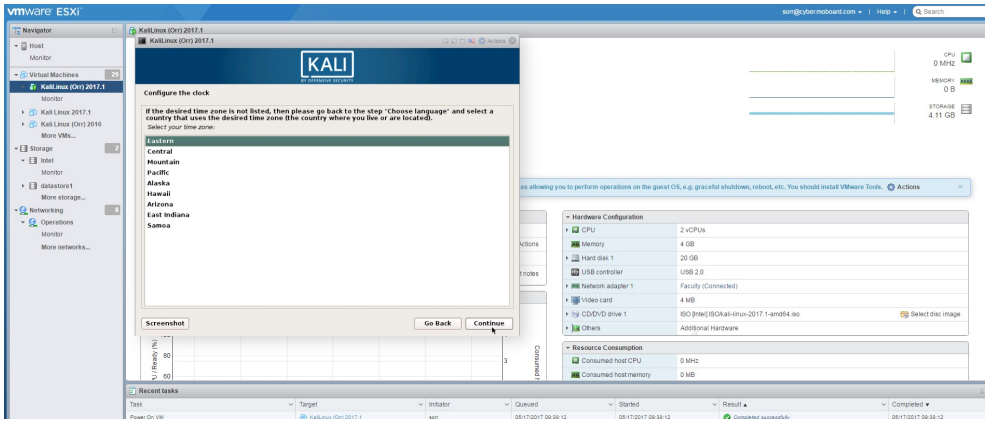
- Select Continue.



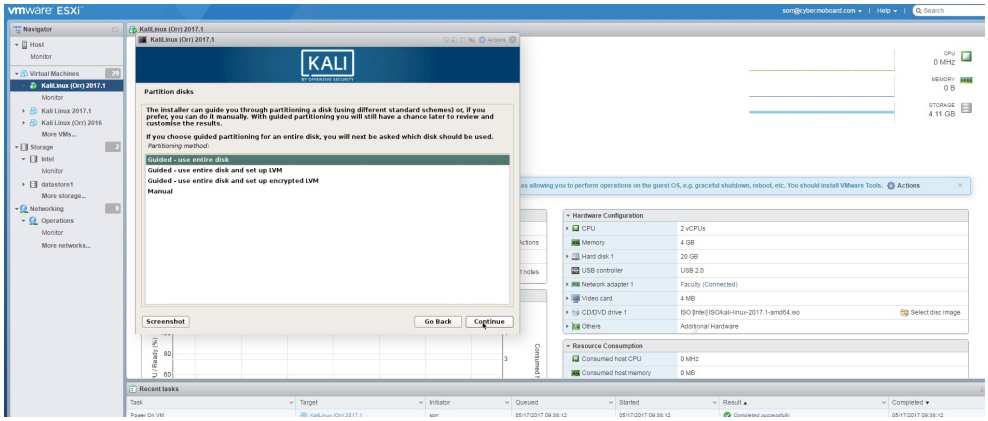
- Enter your password and **do not forget it**. Select Continue.



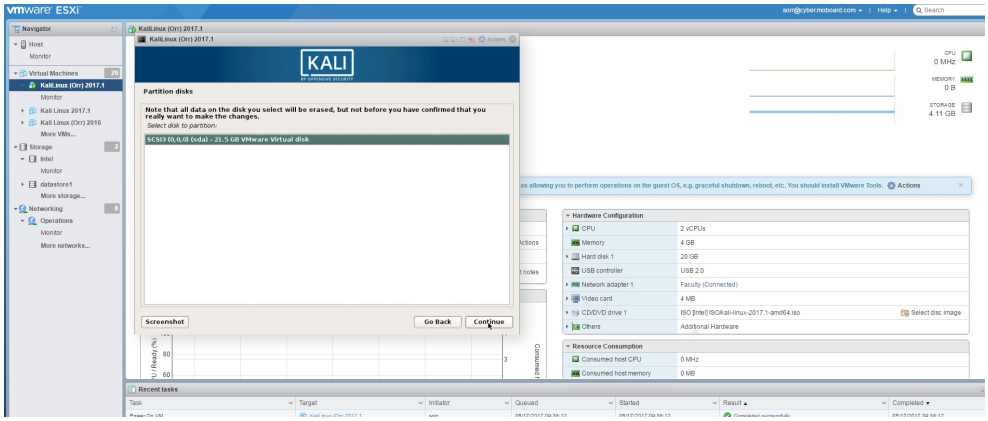
- Select Eastern. Select Continue.



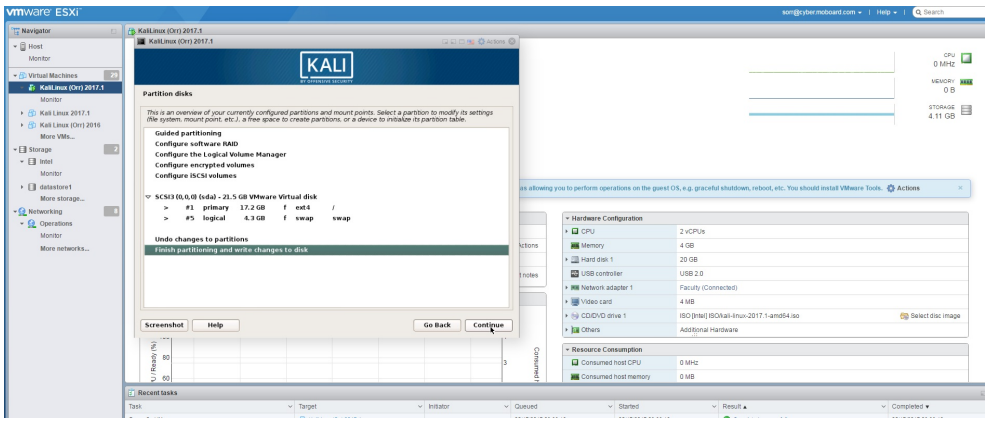
- Select Guided - use entire disk. Select Continue.



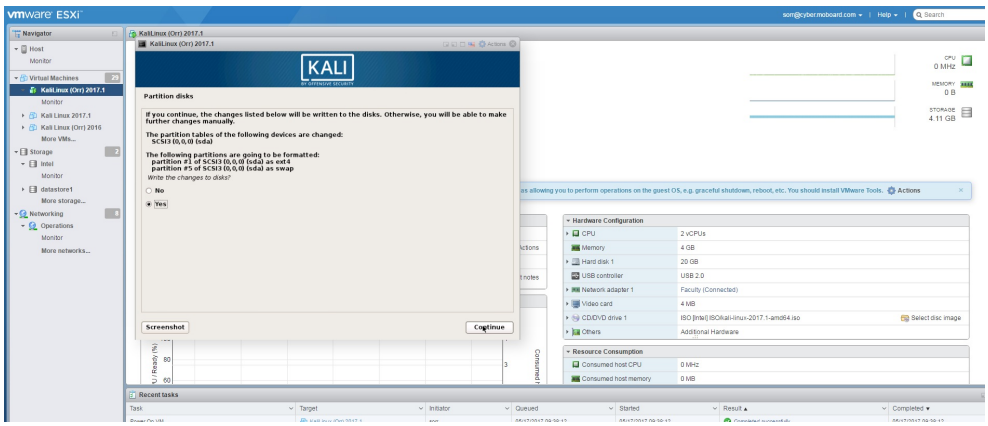
- Select default option (i.e., SCSI3). Select Continue.



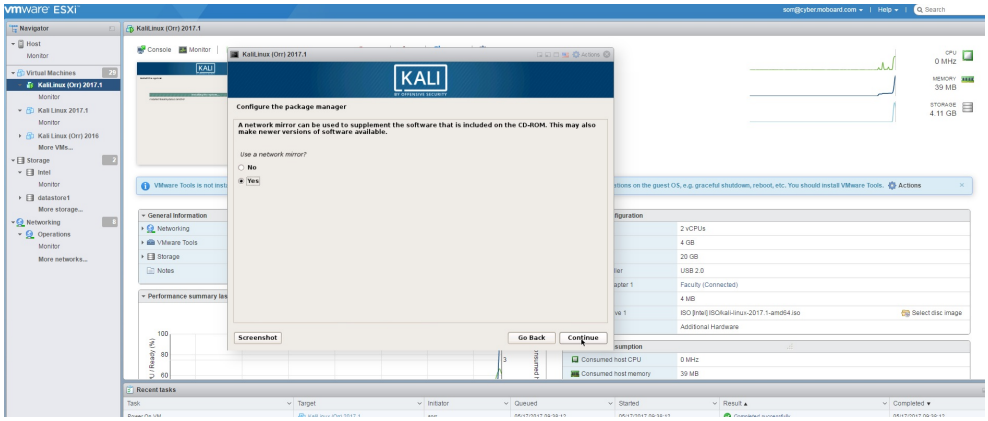
- Select Finish partitioning and write changes to disk. Select Continue.



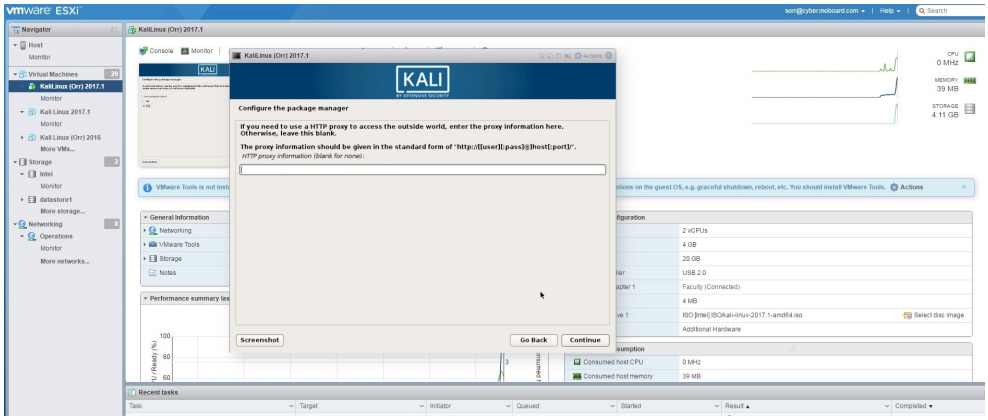
- Select Yes. Select Continue.



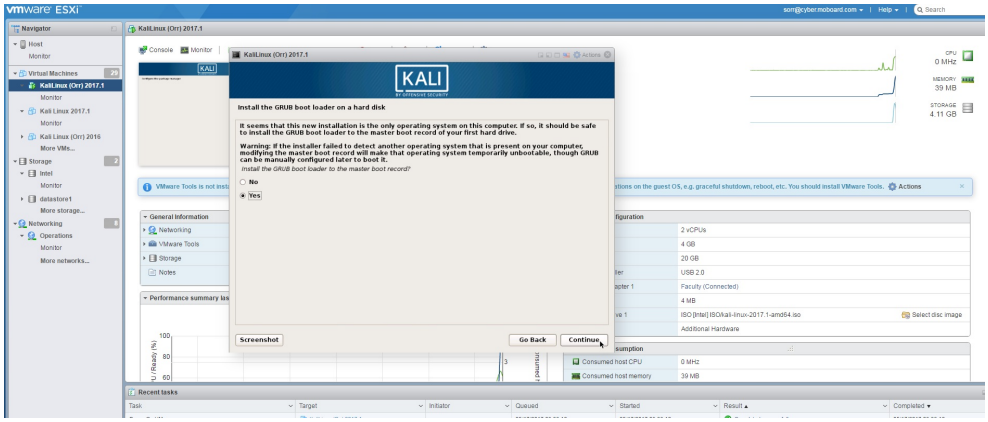
- Select Yes. Select Continue.



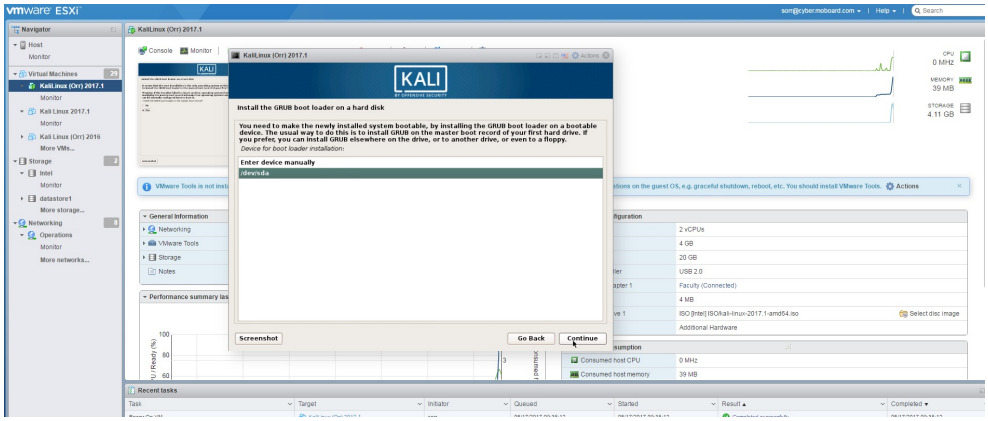
- Select Continue.



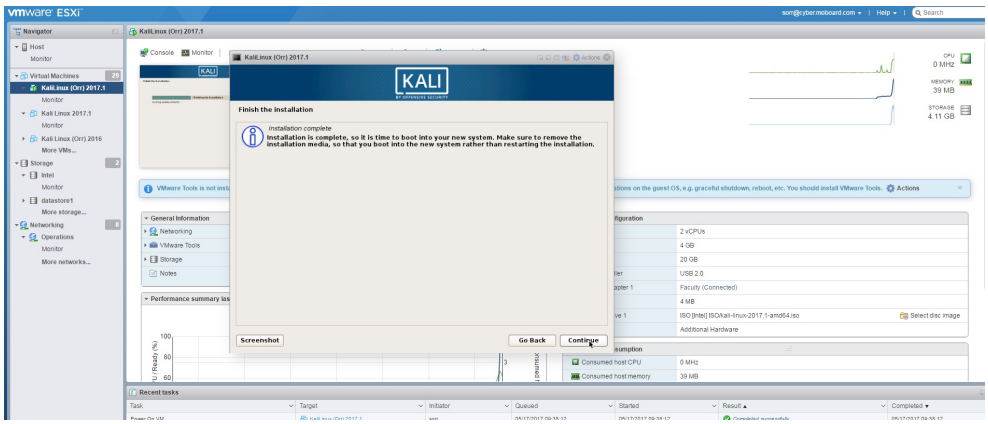
- Select Yes. Select Continue.



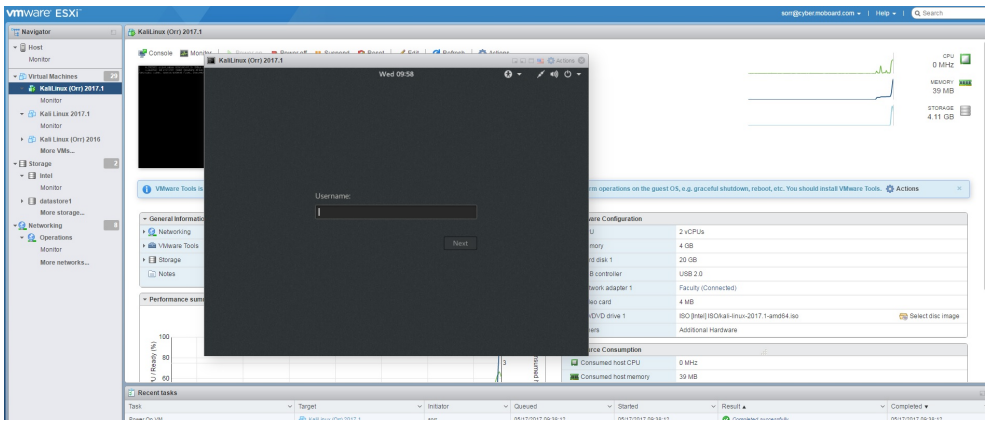
- Select /dev/sda. Select Continue.



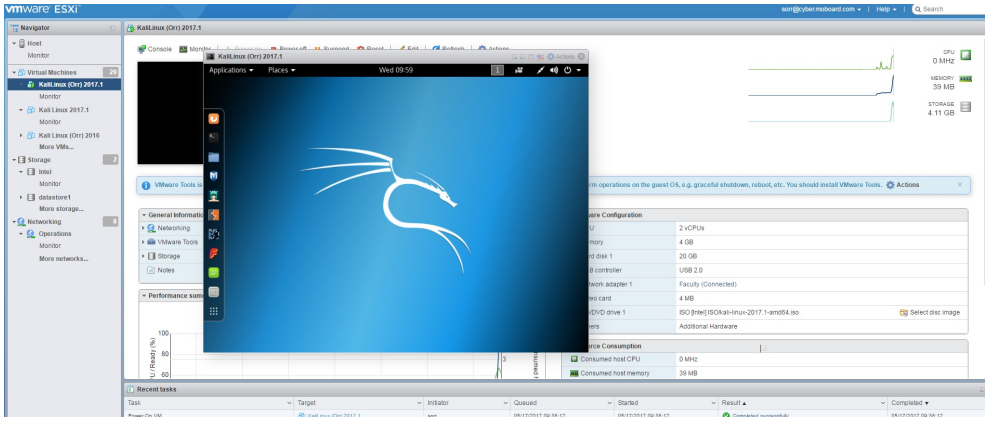
- Select Continue.



- Log in with the username **root** and the password you set (Default password is **toor**)



- Your offensive cyber operations platform (Kali Linux) is installed.



- Open a terminal
- Update the image

```
sudo apt-get update
sudo apt-get upgrade
```

Note: If students do not use the **sudo** command, they will likely get an error message similar to the following:

```
E: Could not get lock /var/lib/dpkg/lock-frontend
```

Use Google to research the fix. It's as simply as removing (hint: rm) the lock file and force package reconfiguration.

References

1. Porter, M. E. (1980, October 01). Competitive Strategy: Techniques for Analyzing Industries and Competitors. Retrieved February 20, 2018, from https://www.hbs.edu/faculty/Pages/item.aspx?num=195

2. Allen, Patrick D., (2009). The Information Sphere Domain Retrieved February 20, 2018, from https://ccdcoe.org/sites/default/files/multimedia/pdf/09_GILBERT%20InfoSphere.pdf

3. Kim, P. (2015). The hacker playbook 2 practical guide to penetration testing. Leipzig: CreateSpace by Amazon Distribution GmbH.

4. Official Kali Linux Documentation. (n.d.). Retrieved February 20, 2018, from https://www.kali.org/kali-linux-documentation/