**CMIT 495 Current Trend and Projects in Computer Networks and Security**

**Week 1 – Virtualization**

1. Access **your AWS** Learner Lab Virtual Environment **and take a screen capture of the AWS Console (Dashboard) and embed it below.**

**A screenshot of a computer

Description automatically generated**

1. **Provide a detailed overview of the steps required to provision (create) and launch an AWS Ubuntu-based server virtual instance. The steps may be listed in bullet points or complete sentences. Use as much space as required.**

* Sign into the AWS Management Console.
* On the top left of the screen lick on ‘services’ and then click on ‘EC2’. This will bring up the EC2 dashboard.
* On the EC2 dashboard click on ‘Instances’ and then click on ‘Launch Instance’.
* On the ‘Launch Instance’ menu this is where a user will create the instance they want to use.
* Choose a name for instance.
* Choose the Ubuntu Server 24.04 (64-bit)
* Choose t2.micro instance type
* Click on ‘Key Pair’ and select ‘Create a new pair key”
* In the ‘create a new pair key’ menu select a name for the key pair.
* Select ‘RSA’ for the key pair type.
* Select ‘.ppk’ for the file format type. Select ‘create key pair’ and the key pair has been created. The .ppk file will download and be stored in the downloads folder.
* Scroll down to ‘configure storage’. Users can keep these settings as default.
* Once these steps are completed click on the ‘launch instance tab’. The instance will launch.
* The instance will launch and then users will see a green banner stating that the instance was created successfully.
* To connect the instance to PuTTy users will have to download the PuTTy application.
* Once PuTTy is downloaded
* One the PuTTy configuration screen enter the host name IP address which will be the IPv4 Ip address. Keep the default port number on 22 and connection type on SSH.
* In the category section, click on the ‘Connection’, >> ‘SSH’ >> ‘Auth’ then ‘Credentials’.
* Complete the following by choosing ‘Browse’, select the .ppk file that you generated for your key pair and choose Open.
* A window will open which indicates that you are connected to your instance.

1. **What are the benefits of virtualization in a cloud environment? Discuss a minimum of three benefits in detail.**

The benefits of virtualization in a cloud environment are its low maintenance, low cost, and ease of use. Users or organizations are not required to maintain the equipment needed since virtualization is available in many locations under the organization's radar. Users/organizations will not have to worry about the upfront costs of virtualization equipment. With platforms such as AWS, providing user interfaces to quickly put up many virtual machines and scale up or down when needed is straightforward.

1. **Based on your experience, what was the most challenging aspect of provisioning and launching the AWS Ubuntu-based server instance in the AWS virtual environment?**

The most challenging part of this process was configuring the EC2 instance with PuTTy using Windows. I also made the mistake of saving the private key file as a .pem and not a .ppk file, so my first three attempts to launch my instance and connect to PuTTy did not work.

1. **Configure your local host computer to use an SSH client application to interact with the newly created and running AWS Ubuntu virtual instance. If using a Windows-based local computer, read over the AWS document, "Connect to your Linux instance from Windows using PuTTY”, download and install PuTTY[[1]](#footnote-1) or use Windows 10 built-in OpenSSH client.**

**A screenshot of a computer

Description automatically generated**

**Ubuntu Instance connection from Windows via PuTTy**

1. **From the local computer establish an SSH connection to the AWS Ubuntu Server virtual instance, login, and update the Ubuntu Server using *sudo apt-get update* and *sudo apt-get upgrade*. Perform a screen capture after having each command successfully run.**

**A screen shot of a computer

Description automatically generated**

**Sudo apt-get update command being executed**

**A computer screen with white text

Description automatically generated**

**Sudo apt-get upgrade command being executed**

1. **Next, describe in depth what the *update* and *upgrade* commands are doing (explain why it is important to run these commands, how often should these commands be run, where do the commands pull the updates).**

The update command is used to update package information from all defined sources; the upgrade command, on the other hand, updates all installed packages to the most recent versions. Using the sudo apt upgrade command will only update existing packages; it will not install new packages unless specific circumstances require necessary dependency resolution. Ubuntu is very useful as it automatically scans for updates and upgrades at least once a week or as often as you set it up to be.

1. **After successfully deploying the Ubuntu Server operating system updates and upgrades, reconnect to the AWS EC2 console, and if needed login again via an SSH client (Note: SSH session inactivity timeout is short). Instructions to SSH are provided by Amazon on how to do so. When connected, run the following commands to obtain information about the host and network settings (perform a screen capture of the results and embed below):**

**A computer screen with text and numbers

Description automatically generated**

1. **What kind of account did you discover when you ran the *whoami* command? How do you**

**know?**

The ‘whooami’ command in Linux is used to display the current user’s username. It is a simple command that tells you the effective user ID the shell is running under.

1. **Note the difference between IP addresses—specifically, when you perform the *ip a show* or *ipconfig* on your personal system, versus the *ip a show* command within the EC2 instance VM command prompt. Describe the network settings of each system. Why are the IP addresses different? Are the IP addresses private or public? What is the difference between a public and private IP address? Explain in detail.**

The IP addresses are different due to the effects of virtualization, which results from each virtual machine having its own virtual network interface adaptor. Similar to VPNs, virtual machines are in private networks. Virtual machines require access to a physical network, which is accessed through what is known as an "uplink." Virtual machines utilize Network Address Translation (NAT) for shared networking. This allows users to configure a virtual machine and external network connection.

When running the ipconfig command on my PC and within an EC2 instance, the resulting IP addresses differ due to the network configurations and environments of the systems. My home router will assign my computer an IP address through Dynamic Host Configuration Protocol (DHCP). In contrast, the IP a show command on an EC2 instance in Amazon Web Services (AWS) reveals an IP address from a Virtual Private Cloud (VPC) subnet, which is also private. However, EC2 instances can be assigned a public IP address for internet access, mapped to their private IP through Network Address Translation (NAT). The difference arises because public IP addresses, globally unique and routable on the Internet, are used to identify devices over public networks.

**A screenshot of a computer program

Description automatically generated**

**‘Ifconfig’ and ‘ip a show’ command executed in the Ubuntu EC2 PuTTy terminal**

**A computer screen shot of a black screen

Description automatically generated**

**‘ipconfig’ command ran on my PC from command prompt**

1. **Virtualization allows us to place the functionality of many servers into a single host while maintaining configurable levels of separation between all virtual machines. How do you believe virtualization could help in data center consolidation? What would you be leery about during and after any transition?**

Consolidation is one of the benefits that comes with virtualization. Virtualization allows its users not to require bare devices to run various services. This allows its users to bring together or consolidate all services and network resources onto one device. Besides the physical advances in virtualization, the data center will be more manageable, scalable, and flexible. Points to be leery about virtualization is how it is a single point of failure. It would be catastrophic if the data center were lost without restoration and disaster recovery in a disaster. It is best to have multiple physical hosts available when hosting a multitude of virtual servers within a host, along with software and backup configurations.

1. **Does virtualization increase the cybersecurity posture of the organization? If so, describe how and why. If not, describe how and why not.**

Virtualization can indeed increase an organization's security posture; it will, however, come with concerns and risks. Using a virtual infrastructure format for centralized storage will help prevent data loss in stolen or compromised devices. When services and applications are correctly isolated, only that specific proportion will be affected in the event of an attack.

1. **There are various virtualization options: bare-metal (Type 1) in which the hypervisors run directly on the hardware as their own operating systems, and user-space (Type 2) hypervisors that run within the conventional operating systems. Which of these options is more secure? Describe the vulnerabilities you believe exist in either Type 1, Type 2, or both configurations. What do you believe can be done to mitigate these vulnerabilities?**

Due to its small structure, hypervisors will only have a small attack surface. However, it will be an issue since all services will run on a single hypervisor, which will cause an ongoing struggle in terms of security and expenses. Despite the small attack surface, it will be very dire if the hypervisor is compromised, resulting in all the attached VMs being compromised. Between type 2 and type 1 hypervisors, type 2 hypervisors take a bigger hit in security than type 1. This is likely because bare-metal hypervisors tend to have access control while host-based hypervisors do not have access. After learning about the vulnerabilities each one possesses, the best way to mitigate the cons of Type 1 is to choose a hypervisor that does not need to separate the management system.

1. **Confirm that you have stopped and terminated your AWS Linux server instance. To confirm, simply type your name below.**

***Jordan Lee***

**References**

Garn, D. M. (2021, August 2). My Comptia Cloud+ Favorites: Virtualization and Resource Management. CompTIA. <https://www.comptia.org/blog/comptia-cloud-virtualization-resource-management>

Garn, D. M. (2021a, June 2). *My comptia server+ favorites: Virtualization and the cloud*. CompTIA. <https://www.comptia.org/blog/comptia-server-topics-virtualization>

1. [↑](#footnote-ref-1)