This week, you’ve covered a lot of ground in your TestOut labs. The goal of the discussion is to get students involved with each other in the learning process. Your instructor may be an expert, but you’re rapidly becoming one!   
  
Sharing what you learn is an important part of learning. It will help you solidify the things you’ve learned, and will help others see things from your perspective.

1. By Wednesday, post your thoughts on the top three things you learned.
2. On Thursday or Friday, read some postings made by classmates and comment on some (at least two) that interest you.
3. On Saturday or Sunday, return and post your replies to the conversation that’s going on. If no one has replied to you, find some other posts you find interesting and join the conversation.

Remember to give substantive explanations of your items. Use professional language and not text speak, just like you will/do in the business world. Don’t forget to have fun!

Hello class,

This week’s topic which I have learnt that are an important part of learning are Security Policies, Risk Management and Business Continuity.

**Security Policies** are written documents that states how a company plans to protect its physical and assets from any intruder. This can be in form of different ways such as the Change in Management Policy, the Physical Security Policy and the Email Policy of the company.

**Risk Management** is the process of identifying, assessing and controlling any threats to a company's investment and its revenue such as financial, accidents and natural disasters. In addition, it can give the company an opportunity to prepare for any problems from this by coming out with a solution.

**Business Continuity** is the planning and the preparing of a company to make sure it overcomes serious incidents such as the disasters and continues its normal operations within a short period of time. This can be in form of establishing a plan B on a different location and using cloud computing system.

***Hello class,***

***This week’s topic which I have learnt that are an important part of learning are Demilitarized Zones (DMZ), Firewalls and Virtual Private Networks (VPN).***

***Demilitarized zone is a physical subnetwork that contains and exposes an organization's external facing services to the Internet which is very dangerous due to security issues. It is like open a room to the public for business without worried what is in that room and what they may take. Most of the unsensitive data is stored there for them to take or browser.***

***Firewalls are network security system designed to prevent unauthorized access to or from a private network. They can be either both hardware and software, or the combination of both. They have been a first line of defense in network security for some time. In addition, they can be in form of hardware or software which is depending what is use for.***

***Virtual Private Networks is a technology that creates a safe and encrypted connection over the internet which is unsafe. It allows users to remote connect to the organization and access the resources and application. It was made to make it easy to allow them to access the resources using the public network which is the internet. Moreover, it allows users who are in the VPN to access those resources***

Hello class,

* This week’s topic which I have learnt that are an important part of learning are Network Access Protection, Wireless Overview and Wireless Attacks.
* **Network Access Protection** is a technology which is used by Microsoft to control the network access of a computer, based on its health. It provides a platform for protecting the access to the private networks of any organization. It gives the system administrators to define policies for the system health which are required. These are the computer ‘s recent operating system, the installed updates and the latest version of the [anti-virus software](https://en.wikipedia.org/wiki/Anti-virus_software)
* **Wireless Overview**. A wireless network is a computer network that uses wireless data connections between network nodes. It is also the transfer of information or power between two or more points that are not connected by an electrical cable. It is a convenience way of sending and receiving data without making any cable connection between nodes.
* **Wireless Attacks** is the kind of an attack by which a trick of a wireless access point is made. It can be done in different form to decrypt and read data that was meant to stay encrypted. The following are the type of wireless attacks, Rogue Wireless Devices, Peer-to-peer Attacks, Eavesdropping, Encryption Cracking, Authentication Attacks and MAC Spoofing

Hello class,

* This week’s topic which I have learnt that are an important part of learning are intrusion detection and prevention, Remote Access, and Network Authentication.

**Intrusion prevention** is a preemptive approach to network security used to identify potential threats and respond to them swiftly. An **intrusion detection** system is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Some intrusion detection systems are capable of taking actions when malicious activity is detected, including blocking traffic sent from suspicious [IP addresses](https://searchwindevelopment.techtarget.com/definition/IP-address). These two can be a good thing if they work hand in hand because it would provide the best network which is properly protected.

**Remote access** is the ability to access a computer from a remote location using ether a home computer or an office network computer. It allows employees to work at home or in another location and be able to have access to a distant computer or network, such as the office network.

**Authentication** is the process of giving individuals access to system objects based on their identity. It ensures that the person is who he or she claims to be. but says nothing about the access rights of the individual. It is a security process required when a computer on a network tries to connect to the server in order to use its resources. It is done by asking the users for some information like entering a valid username and password. If the user's identity has been stored by the server, then the connection process is allowed

Hello class,

* This week’s topic which I have learnt that are an important part of learning are Cloud Services, Malware and Audits.

**Cloud Services** are services which are made available to users on demand through the Internet from a cloud computing provider’s server instead of being provided from a company's premises servers. There are many services provided by the cloud which are IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-Service), Storage level which can be in, Database, Information, Process, Application, Integration, Security, Management, and Testing-as-a-service.

**Malware** is a software which is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It is intentionally designed to cause damage to a computer, server, client, or computer network. It does the damage after it is introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The best software to protect from this is by using the Malwarebytes

**Audits** are the systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern. The above definition is on the account point of view. A network security audit on the other hand is a way of determining the effectiveness of network security to resolving underlying network security issues. They are critical ways of understanding how well any organization is protected against security threats which can be internal or external.

Hello class,

* This week’s topic which I have learnt that are an important part of learning are email security, authentication, and authorization,
* **Email security** is the description of various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise. The main purpose of this is to prevent the data from malware and viruses which can advanced threats like email phishing, email security issues. This can lead to breaches that cost millions of dollars in lost business and damage to your reputation.
* **Authentication** is the process of verifying who you are, which can be the confirmation of your own identity. To put it in another way, it is the process that confirms a user’s identity. This is done by entering a username and password which allows the system to confirm their identity after confirming it from the database of the server of the website they are visiting.
* **Authorization** is the process of granting access to the system. To simplified this, it is the process of verifying what you have access to. Moreover, it is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. It is also the process of giving someone permission to do something.

This week’s topic which I have learnt that are an important part of learning are Linux Users, Linux Groups and Group Policy.

* **Linux Users** are anyone’s who use a Linux computer. They are identified by a number called unique identification number. The Linux system has two types of users which are the super user and normal users. A super user can access all the files, while the normal user has limited access to files. A super user can add, delete and modify a user account. They can be created using the useradd command.
* **Linux Groups** are mechanism to organize a collection of users. They are identified by a number called the GID. There are two types of groups which are a primary group and a supplementary group. Each user is a member of a primary group and of zero or ‘more than zero’ supplementary groups. They can be created using the groupadd command. In addition, groups organize collections of accounts, primarily as a security measure.
* **Group Policy** is a feature of Microsoft Windows active directory that adds additional controls to user and computer accounts. The policies give a centralized management and operating systems configurations of user’s computing environments. In addition, there are method of securing user’s computers from data breaches. The give the system administrators the abilities to protect, secure, and lock down computers and user accounts.

Hello class,

This week’s topic which I have learnt that are an important part of learning are *Data Management Symmetric Encryption and Asymmetric Encryption.*

* ***Data Management*** *is an administrative process which is involves in acquiring, validating, storing, protecting, and processing required data to ensure the accessibility, reliability, and timeliness of the data for its users. It is also the disciplines related to managing data as a valuable resource. This is done by many organizations to make sense of the vast quantities of data that they are gathering, analyzing, and storing.*
* ***Symmetric******Encryption*** *is a method of cryptography where a single key is responsible for encrypting and decrypting data. The keys may be identical or there may be a simple transformation to go between the two keys Its drawback is that all parties involved must exchange the key used to encrypt the data before they can decrypt it.*
* ***Asymmetric Encryption*** *is the process of using two keys to encrypt a plain text. It is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Secret keys are exchanged over the Internet. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and therefore asymmetrical encryption uses two related keys to boosting security. A*[*public key*](https://www.ssl2buy.com/wiki/what-is-a-public-and-private-key-pair/)*is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know. In additional, a message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet.*

***Hello class,***

***This week’s topic which I have learnt that are an important part of learning are Redundancy Backup and Restore, and Cloud Storage***

***Redundancy of data is a condition created within a data storage technology in which the same piece of data is held in two separate places. This can mean two different spots in multiple software platforms. Whenever data is repeated, this basically constitutes data redundancy. This can occur by accident but is also done deliberately for backup and recovery purposes.***

***Backup and Restore. Backup is the process of backing up, refers to the copying into an archive file of computer data that is already in secondary storage so that it may be used to restore the original after a data loss event. In other words, it is the one that serves as a substitute or support. Many companies back up data they deem to be vulnerable in the event of data corruption, hardware failure, malicious hacking, user error or other. There are three types which are full backups, incremental backups and differential backups. While Restore is the process of bring back to or put back into a former or original state. System Restore is a feature in Microsoft Windows that allows the user to revert their computer's state to that of a previous point in time, which can be used to recover from system malfunctions or other problems.***

***Cloud Storage is a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers which can be in different locations, and the physical environment is owned and managed by a hosting company. This is like a storage unite where we keep our house hold goods.***