COMPTIA ---6

summarizing Routing and switching use cases

:::Prevent switching loops you do this by impementing stp or rstp on switches
:::preven bpdu attacks a bpdu guard enabled on edge ports of a switch will preven bpdu attacks.
''::prevent unauthorized users from connecting to unused ports

SImple network management protocl version 3
(SNMPV3"

------MONITORS AND MANGES NETWORK DEVICE..SWITCH ROUTERS.

ADMINISTRATORS SUE SNMPV3 TO MANAGE AND MONITOR NETWORK DEVICES AND SNMP USES UDP PORTS 161 AND 162 SNMPV3 ENCRYPTS CREDENTIOALS BEFORE SENDING THEM OVER THE NETWORK AND IS MORE SECUREE THAN EARLIER VERSIONS.

agents on clients can be either permanent or dissolvable a permanent agent sometimes called a persistent NAC agent removes themselves immediatelhy after they report back to the nac system

A agentless NAC system scans a client remotely without istalling code on the client either permanently or temporarily

**pap---password authentification protocol is used with point to point ppp ** to authenticate clients.ppp primarily used with dial-up connections

PAP AUTHENTICATION USES A PASSWORD OR PIN A SIGNIFICANT WEAKNESS IS THAT PAP SENDS THE INFORMATION ACROSS A NETWOK IN CLEARTEXT MAKING IT SUSCEPTIBLE TO SNIFFING ATTACKS CHAP IS MORE SECURE THAT PAP BECAUSE CHAP DOESNT SEND PASSWORDS OVER THE NET IN CLEAR TEXT..

challenge handshake authentication protocol chap ALSO USES ppp and authenticates remote users but is more secure that pap.

Radius remote authentication Dial in User service radius is a centralized authentication service instead of each individual vpn server needing a seperate database to identify who can authenticate. the vpn servers forward the athentication requests to a central radius server.

TACACS+ terminal access controller access control system plus.---------------- is an alternative to radius and it provides two essential security benefits over radius first it encrypts the entire authentifcation process. where radius only encrypts pw.

**radius and tacacs+provide centralized authentication radius only encrypts the pw by default but can be used with eap to encrypt entire sessions. tacacs+ encrypts the entire session by default and can be used with kerboros.

aaa protocols provide authentication authorization and accounting. accounting tracks user access with log servives.**

**summarze virtualization concepts. **

HYPERVISOR::::: THE SOFTWARE THAT CREATES RUNS AND MANAGES THE VMS IS A HYPERVISOR. SEVERAL VIRTUALIZATION TECHNOLOGIES CURRENTLY EXIST INCLUDING VMWARE PRODUCTS MICROSOFT HYPER V PRODUCTS.

HOST:::::::::; THE PHYSICAL system hosting the vms is the hsot. it reqires more resources than a typical system. such as multiple processors massive amounts of RAM, FAST, AD ABUNDUNT, AND DRIVE SPACE.

GUEST:::OPERATING SYSTEMS RUNNING ON THE HOST SYSTM ARE GUEST OR GUEST MACHINES.

Host scalability:::: scalability refers to the ability to resize the computing capacity of the vm you do this by assigning it more memory, processors and disk spce.

host elasticit refers the ability to dynamically change resources assigned to the vm based on the load.

a THIN CLIENT Is a computer with enough resources to boot and conendct to a serve to run specifica applications or desktop..

Container virtualization runs services or applications within isolated containers or application cells.

VM escape is an attack that allows an attacker to access the host system from within the virtual system.

VM sprawl accurs ehan an organization has many vms that arent appropriatelyy managed most organizations have specici policies in place to ensure physical servers are kept up to date and personnel only make changes.

**Virtualization allows multiple virtual servers to operate on a single physical server providing cybersecurity resilience with lower operating costs keeping systems up to date with current patches is the best protection from vm escape attacks.

**

replication.... vms are simply files.. that have complexity.. vms is jsut a group of files. they are easy to replicate. snapshot.... a copy of a vm a moment in time.
Non persistency. .. persistent virtual desktop each user has a custom destop imager.. and secure

systems design conceps help ensure that computing systems are deployed and maintained in a secure state .
Endpoints security.. computing devices such as servers desktops laptops mobile device IOT devices endpoint detection adn respoinse. endpoint threat detection and etdr. provides contionious monitoring of endpoints.

**endpoint security, hardening systems and configuration management,

secure baseline and integrity measurements**
--Initial baseline configuration. use various tools to deploy systems consistently in a secure state.
integrity measurements for baselin deviation.
.. automated tools monitor the systems for any baseline chanes..

remediation.. NAC network access controls can detect some changes and automatically isole.
342
Usint master images for baseline configuration

Secure starting poing the image includes mandaed security configurations for the systm
Reduced consts. deploying imaged systms reduces the overall maintenace costs and reliability.

A master image provides a secure starting point for systems. administrators sometimes create them wih templates or with other toosl to create a secure baseline they then use integrity measurrement sto discover when a system deviateds from the baseline

Patch management.... ensures that sysems and apps stay up to date with current patches.

**Patch management procendures ensure that operating systems, applications, and firmware are p to date with current patches. this protects the systems from known vulnerablities. change management defines the process and accounting structure for handling modifications and upgrades. the goals are to redce reisks related to unintended outages and provide documentation for all changes.* *

Application approved lists sometimes called whitelists and block lists (someties called application deny lists or black lists. are two additional methods used as endpoing security solutions..

an application ALLOW LIST is a list of apps authorzed to run on a system. In contrast, there is a block list,

**An application approved list is a list of authorized software and it prevents users from installing or running software that isnt on the list an application block list is a list of unauthorized software and prevents users frp, omsta;;omg pr rimmomg software on the list.

**

**Application programming interfaces.. api, is a software component that gives developers access to features or data within another appliction service or an OS Its common for developers to use APIS with web application IOt devices and cloud based devices.

APIS are susceptible to attacks so developers need to address sever api condiderations.

authenticationnn will prevent unauthorized entities from using the APIS.

authorization methods to secure access to the api, developers may have one level of access.

transport level secuirity the API should use strong security such as tls

MICROSERVICES AND APIS MICROSERVICES ARE CODE MODULES DESIGNED TO DO ONE THING WELL. THY ARE TYPICALLY SMALL CODE MODULES RECEIVE A VALUE AND RESPOND WITH A VALUE fULL dISK ENCRYPTS an entire disk several apps availabile many vendors now manufacture self encrypting drives seds also known as hardware based fde drives seds include ncryption circuityr built into the drive these typically allow usersto ender credetials. ****

**A self encrypting drive SED automatically encrypts and decrypts data on a drive without user intervention. an opal compliant drive requres users to ender credentials to unlock drive wihen booting system.

BOOT INTEGRITY these processes verify the integrity of the os and boot loading systems. ex. can verify that keyp operating system files haven't been changed. *

many organizations implement the boot integrity processes t

BOOT security and UEFI

"""**basic Input output Services = Bios.** includes software that provides a computer with basic instructions on starting. It runs basic checks locates the os. and boots. the bios is a hardware chip that you can physically see and touch. combination of hardware and software is firmware. Newer systems use Unified Extensible Firmware Interface. """""overwrites by flashing. *TPM trusted platform Module is a hardware chip on a computers motherboard that stores cryptographic keys used for encryption. many compters include tpm and you may see them on mobile devices.

Boot attestation process. when the tpm is configured it captures signatures of key files used to boot the computer and stores a report of the signatures secuerly THe second secure boot chcks the files against the stored signatures to ensure they havent been changed. if it detects files that have been modified. it blocks the boot process. n

A **remote attestation** works like secure boot ...however instead of checking the boot files against report stored in tpm it ses a seperate systm..

a hardware security module is a security device you can add to a system to manage generate a securely starting point

a microsd hsm is a microsd card that includes an HSM a microsd card is small at 15 mm long x 11 mm microsd slot with an adapter you can install any microsd card into an sd card slot,,
**a hardware security module hsm is a removable or external device that can generate store and manage rsa keys used in a asymmetric encryption many server based applications use an hsm to protect.

**Data is one of the most valuable resources any organization manages second only to its people.

Data loss prevention dlp tecniques and technologies to prevent data loss can block the use of usb flash drives and control the use of removable media

RIghts management often called digital rights management refersto the technologies used to provide copyright protection for copywrited rowrk. ..
removable media refers to any storgae system that you can atach to a compter.

Data exfiltration is the unauthorized ransfer of data outside an organization and is a signifcant concern in some cases
Data exfiltration is the unauthorized data out of a network Data loss prevention techniques and technologies can block te use of usb devices to prevent data loss and monitor outgoinf email traffic for unauthorized data transfers.**

THe **primary methods of protecting the confidentiality of data ar with encryption and strong access controls.. database column encryption protects indidvidual fiels within a database..****

database security.. oracle database or microsoft sql can encryp data held a a database

cloud computing computing resources other than your local computer.

SAAAS SOftware as a service. inludes any software of application provided to users over a network such as the internet.. Internet users access the Saas applications with a web browser It usually doesnt matter which web browser or operating system a SAAS customer uses.. any web browser. as mentioned before.. we based email. is an example of SAAS .. gmail yahoo.. ex..

**Applications such as web based email provided over the internet are software as a service cloud based technologies Platform as a service provide customers with a fully ,anaged platform including hardware operating systems and limited applicatios.. the vendor keeps systmes up to date with current patches. **

Platform as a service provides customers with a preconfigured computing platform they can use as needed . It provides the customer with an easy to configure operating system combined with appropriate applications and on demaind computing.

Infrastructure as a service IAAS allows an organization to outsource its equipment requirementsincluding the hardware and all support operations. the Iaas service provider owns the equipment. houses it in its data center and performs all the required hardwaqre maintenace.

**IIas provides customers with access to hardware in a self managed platform anything as a service refers to cloud based services other than saas , paas, or iias, xaas, includes services such as communications databases desktops storage security and more.

Private clouds are only available for one organization.
**

xaas anything aws a service refers to cloud services beyond saas , paas and iaas xaas includes a wide assortment of services that can be delivered via the cloud..

Public cloud services are availabel from third party companies such as amazon google microsoft and apple they provide similar services to anyone willing to pay for them ..

Private cloud. is set up for specific organizations for example the shelbville nucluear power plant might decide it wants to store data in the cloud. ....

managed security service provider... a third party vendor that provides security services for smaller companies. many small companies ***

patch management vulnerability scanning ,spam and virus filtering, data loss prevention, virtual private network connections,proxy services for web content filtering. intrusion detection

a mssp may sell aplliances.
**

a MSP provides any it services needed by an orgainzation including security services provided by a mssp

csp cloud service provider.

Cloud Security Controls

High availability and high availability across zones. --High availability indicates a system or service remains operaitonal with almost zero downtime. typically achieved by using multiple load balancing nodes.

resource policies

**high availabilibility and *high availability across zones.. indicates a system service that remains oeperational*

high availability
Resource policies. in this context resources refer to cloud based resources such as folders projects and virtual machine instances.

secrets management... secrets refer to passwords and encryption keys that users create a secret management system stores and manages secrets.

i**ntegrating and auditing** the csp integrates security controls into the cloud based resources..

permissions identify who can access the data

encryption protects the confidentiality of data the csps commonly provide encryption.
virtual private cloud endpoints

replicaton.. data replication is the process of copying and storing data.

virtual network.

public and private subnets..
security groups

Dynamic resource allocation
Instance awareness
virtual privae cloud endpoint is a device within a virtual network where users can connect to the vps endpoint then access other resources.
**TRANSIT GATEWAY
**CONTAINER SECURITY

ON PREMISES AND OFF PREMISES.

**CSP EMPLOY NATIVE CONTROLS TO PROTECT CLOUD BASED RESOURCES.
**CLOUD BASED DLP ---CAN ENFORCE POLICIES FOR DATA STORED IN THE CLOUD SUCH AS ENSURING THE PERSONALLY IDENTIFIABLE INFORMATION IS ENCRYPTED.

segmentation..
nEXT generation securegateway
swg is a combination of a proxy server and a stateless firewall the SWG is typically a cloud based service but it can be ona site applieance .. it fileters traffic to prevent threats.

**A cloud acces ssecurity broker casb, is a software tool or service deployed between an organization network and cloud provider it provides security by monitoring trafffic and enforcing security policies a next generation secure web gateway provides proxy services for traffic from clients to internet sites.. such as filtering urls and scanning malware.

Firewall considerations.
... vns need firewalls..

IAC Infrastructure as code refers to managing and provisioning data ceters with code to define vms and virtual networks.

**SOftware defined network sdn uses virtualiztion technologies to route traffic instead of using hardware routers or switches. **

oftware defined visibility sdv refers to technologies used to view all network traffic. as an orgainzation uses mrore cloud based resources some network traffic may bypass security devices. n
Hardware routers use rules within the acl to identify whether a router will forward or block traffic on the data plaane this is always propritetary bc it is implemented on specific hardware routers.
Routing protocols such as open shortest path first OSPF and Border Gateway Protocol bgp, help routers determine the best path to route traffic on the the control plane.

**Software defined visibility sdv refers to the technologies used to view all network traffic. as an organization uses more cloud based resources some network traffic may bypasss security devices. **

**Edge and Fog computing.. is the practive of storinga nd processing data close to the devices that generate and use the data in the cloud requiring round trips to retrieve the process data..

as an example... autonomous technologies in automobiles.

cloud security alliance
;;;THe csa is notfor profit organization that promotes best practives related to the cloud. Its member based organization.

nistsp800124 are the guidelins for monitoring mobile devices.

Deployment models ....for mobile devices.

**corporate owned
.... organization issues to employees.
**COPE corporate-owned personally enabled . is similar to the traditional corporatte owned model.

BYOD.
Bring your own device to avoid some of the challenges related to supporting any possible mobile devices some organizations

Corporate-owned,personally enabled devices are owned by the organization but employees can use them for personal reasons a bring your own device policy allows employees to connect their own personal devices to the corporate network a choose your own device policy includes a list of appoved devices that employees can purchase and connect to the internet.

connecgion methods and receivers.
**cellular
**wifi
**bluetooth
**nfc near field comm
**rfid radio frequency identification

**rfid radio frequency identification.
.infrared. .. line of sight wireless tech
USB Universal serial Bus.. mobile devices can typically connect to a desktop pc of laptop via usb
**point to point betwween two wireless devices.

**Point to multipoint. .. apoint to multipoint connection creates an ad hoc network... in ad hoc mode
Mobile Device Management.
includes the tech to manage mobile devices the goal is to ensure these devices have security controls in place to keep them secure some vendors sellunified endpoint management solutions to manage mobile devices.

uem tools ensure systems are kept up to date with current patches have antivirus software installed with upt to date definitions and secured using standard security practices.

**Application Management.. mdm tools can restrict what applikcations can run onmobile devices..
**

***full device encryption protects agains the loss of confidientiality.

***storage segmentation. In some mobile devices its possible to use storatge segmentation to isolate data.. for example users might be required to use external storage for any corproate data toreduce the risk of data loss

**Content management. After creating segmented storage spaces, its important to ensure that appropriate content is stored there.

Containerization.
Passwords and pins
**Biometrics
**Screenlocks

***Mobile Device management tools help enforce security policies on mobile devices. This includees the use of storage segmentation containerization. and full Device encryption to protect data. Containerization is useful when using the byod model they also inclued enforcing strong authentication methods toprevet unauthorized users.