M T W T F S S
Page No.: YOUVA
Date:

11/09/2022 (W5)

Module-2 Cyber Security Roles, Process and Operating Systems Security

⇒ IT Security

- protection of computer systems from theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.

⇒ Cyber Security Analysts should have:

- Technical skills → OS knowledge, database knowledge, cross-site scripting, malware, DDoS and general Cyber Sec knowledge -
!! around firewalls and antivirus

- Soft~~ware~~ Skills → effective communication, critical thinking, motivation to solve problems.

⇒ Security Standards and Compliance

- Best practices, baselines and frameworks

• Used to improve the controls, methodologies and governance for IT departments or the global behaviour of the organization.

- Seeks to improve performance, controls and metrics
- Helps translate business needs into technical or operational need.

-Normative and compliance : compulsory to comply.

↳ Best practices, frameworks and others

- COBIT
- ITIL
- ISOs
- COSO
- Project management methodologies
- Industry Best practices
- Developer recommendations
- Others

↳ Cobit - control objectives for information and related technologies (to bridge gap between technical issues, business risk and control requirements)

↳ ITIL - Information Technology Infrastructure Library. (best practices for delivering IT Services) (Standardizes selution, planning, delivery and support of IT Services to maximize efficiency)

↳ ISO - International organization for standardization)

↳ COSO - operations reporting and Compliance.

M T W T F S S

Page No.: YOUVA

Date:

⇒ potential Roles : Information Security Analyst
: Chief Information Security officer (CISO) :)

⇒ Business process management

- set of defined, repeatable steps that take inputs, add $ value, and produce outputs that satisfy a customer's requirements.

↳ Attributes of process

- Inputs
- Outputs
- Bounds / Scope
- Tasks / Steps

↳ ITIL Lifecycle

- Service Strategy - continual service strategy
- Service Design - designing new services, changes to existing ones
- Service transition - build and deploy IT services, existing service changes, etc
- Service operations - steady state, monitoring and ensuring.
- Continual Service Improvement - Continually reviewing metrics, test & prioritize and implement improvements.

M T W T F S S
Page No.:
Date:
YOUVA

↳ Selut ITIL processes

- problem management
- Change management } operational processes
- Incident management }
  - Incident is an unplanned interruption to an IT Service, a reduction in quality of an IT Service, and/or failure of a configuration item.
  - phases →

    log > assign > track > categorize > prioritize > resolve > close
- Event management.
- Service level management
  - planning, coordinating, drafting and monitoring and reporting on Service level Agreements (SLAs)
- Information Security management.
  - maintaining ISP and specific security policies.

→ Event management, Incident management, problem management

Service operations

⇒ CIA Triad (W2)

⇆ 3 key objectives of Network Security

- Confidentiality → preserving authorized restrictions on information acess and disclosure.
- Integrity → guarding against improper information modification or distruction.
  → ensuring information non-repudiation and authentidity
  ↓
  can't challenge that a transaction ocurred.
- Availability → Timely and reliable acess to information.
  → loss of availability : distruption of acess to an information system.
- Authenticity → property of being genuine and verifiable
- Accountability → mapping actions to an identity.

⇒ Notable websites

- https://www.securityforum.org

M T W T F S S
Page No.:
Date:
YOUVA

⇒ Identification and AAA

Identification ⟶ Accountability, Authentication, Authorigation

↳ In order to use a resource :

① Identification
↳ ② Authentication
↳ ③ Authorization
↳ Resource
↳ ④ Accountabil

↳ Authentication methods : something that we have (ATM)
: Something that you know (PIN)
: Something you are (fingerprint)
(Biometrics)
↳ Biometric Capture → imag prowsin
→ bits/bytes translation → C
template extraction → Biometric
matching

⇒ Controls

- Administrative (policy or proudure)
- Technical (firewall)
- Physical (seperate rooms, vault)

↳ Each control type can be:
- corrective (policy, training, penalty for breaking procedures)
- preventive (internal audits)
(prevent or uncover violations of internal controls)
- Dissuare (camera in a server room)
- Recovery (backups)
- Detutive (identify possible violations)
- Compensatory (identify a gap, if admin control wasn't able to)

[persuade not to take particular action]

⇒ Acess Control

- keeping track of who has acess to resource.

↳ models:
- MAC - Mandatory Acess Control
  - ↳ use labels to regulate acess
  - ↳ Military use
- DAC - Discretionary Acess Control
  - ↳ Each object (folder/file) has an owner and owner defins rights and privilege.
- Role based acess control
  - ↳ Configs based on user Roles
  - ↳ ex: management group, sales group, etc.

- Centralized
  - ↳ SSO
  - ↳ provide 3As
- Decentralized
  - ↳ independent ~~access~~ access control methods
  - ↳ local power
  - ↳ used in military in battle

↳ Best practices for access control field

- least privilege
  - information access limit
- Seperation of duties
  - verify employee activity
- Rotation of duties
  - Tracking and control

⇒ Access Control methods

↳ physical : perimetral
: Building
: work areas
: Servers and networks

⇒ Technical uses of physical security controls

- ID Badges
- list and logs
- Tokens
- Tramps
- Cameras
- proximity Sensors

↳ logic : ACL (Routers)
: GPO's → group policy Object
- password policies
- Device policies
- Pay time restrictions
: Accounts
- centralized
- Decentralized
- Expiration

↳ Monitoring auss Control procus

- IDS (Intrusion detection system) - detects
- IPS (intrusion prevention system) - kills
- HOST IDS and IPS (host based detection or prevention sys)
- Honey POT (While attacker in honeypot, all traffic and techniques
- Sniffers (packet analyzers - monitors traffic) are being reviewed)

W3

⇒ MS Windows Components

- User mode and Kernel mode
- Drivers call routines that are exported by various kernel components

↳ User mode

- When one starts a user-mode application, windows creates a process for the application.
  - private virtual address space
  - private handle table.
- Each app runs in isolation

↳ Kernel mode

- All code that runs in kernel mode shares a single virtual address space.
- If a kernel-mode driver crashes, entire operating system crashes

⇒ file systems and Directory structure

- NTFS (New technology file system)
- Fat xx (File allocation table)
  - ↳ xx refers to no. of bits used to enumerate a file system block.
- used for 32 gigs and below storage devices (USB)

Directory structure

!!

C:
- \PerfLogs (Hidden) - performance logs
- \Program files - holds 64 bit applications
- \program files (x86) - holds 32 bit applications
- \programData - accessed by computer programs
- \Users - user profiles stored here
  - \public - multiple user shared folder
  - \Username\ - specific user directory
    - \AppData - application data specific to user
- \Windows - windows stored here
  - \system - stores 16 bit DLL's
  - \system32 - system files needed to run windows stored here
  - \SysWow64

Stores 32/64 bit DLLs - \system32
Stores 32 bit DLL - \SysWow64

→ Dynamic link library - shared library concept.

→ collection of small programs that larger programs can store when needed to complete specific tasks.

M T W T F S S
Page No.:
Date:
YOUVA

⇒ Linux

↳ Kernal : Core of OS, designed to interact directly with hardware
: manages system and user input-output, processors, files, memory and devices

↳ files and directories

↓ represented by "-" in CLI

↳ represented by "d" in CLI

⇒ /Root not same as /
/root is home directory of root

⇒ /bin contains binary executables
- Ps, ls, ping, grep, cp, mv, etc

⇒ /sbin contains system maintenance binary executables.
- Iptables, reboot, fdisk, ifconfig, etc

⇒ /etc contains configuration files of all programs

⇒ /var that are expected to grow/change constantly
- /logs contained in /var

⇒ /tmp contains temporary files
- deleted when system reboots

⇒ /home is home directory for all users.
- personal files stored here

⇒ /boot contains boot loader files used during boot time.

M T W T F S S
Page No.: YOUVA
Date:

⇒ Run levels

Run level	Name	Description
0	Halt	Shuts all services for shutdown
1	Single user	Used for system maintenance, No network, capabilities
2	Multi User	used for maintenance and sys,
3	Multi User	Non GUI, operations for testing server systems
4	–	Custom Mode, used by SysAdmin
5	Graphical X11	Graphical login with same usability of 3
6	Reboot	Shuts all services for Reboot

⇒ Files and directory permissions

- Users, group and Everybody
  - Read (r) : 4 (100)
  - Write (w) : 2 (010)
  - Execute (x) : 1 (001)

Ex:

-rwxr-x---

- -rwx → user has full perms
- r-x → group has r and x perms
- --- → everybody has no perms

M T W T F S S
Page No.:
Date:
YOUVA

↳ change permissions

- chmod <permissions> <filename>
- chmod 755 <filename>
- chmod u=rw, g=r, o=r <filename>
  - u → user
  - g → group
  - o → others

↳ change owner

- chown <user>:<group> <filename>
  - both user and group owns the file

!!

⇒ PentestMonkey : site that pentesters access to get cheat sheets and understand vulnerabilities and fixes.

⇒ MacOS auditing

↳ About myMAC menu Settings gives details about MAC OS (in apple menu)
↳ Activity monitor gives information about all and any active process
↳ Console is MacOS's application for logging any and all information

↳ the security and privacy setting

- Under the line is something called gatekeeper - prevents unauthorized apps from being installed.

- filevault is macOS's encryption which encrypts your entire hard drive
- firewall option allows to block all incoming connections
- startup disk shows any partition that's on interval drive and all connected or network drives.
  - ↳ can boot into target disk mode which turns active computer into an external drive to show up to another network device.

↳ hidden partition called macOS Recovery (gets deleted if disk is formatted)

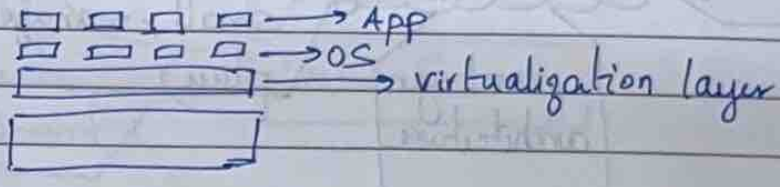
↳ Reinstall macOS doesn't delete and reinstall the OS, it just replaces os files which doesn't touch user directories (personal data shouldn't get compromised)

M T W T F S S
Page No.:
Date:
YOUVA

W4
12/9/2022

⇒ Virtualization

- Allows you to create multiple simulated environments or dedicated resources from a single, physical hardware system.
- eg: VM / Guest
  Hypervisor / Host



Virtualization Architecture

↳ Hypervisor is the software or application that runs on actual ~~harddrive~~ hardware that allows virtualized OSs.
↳ VM / Guest is anything virtualized on top of hypervisor.

⇒ Cloud deployment

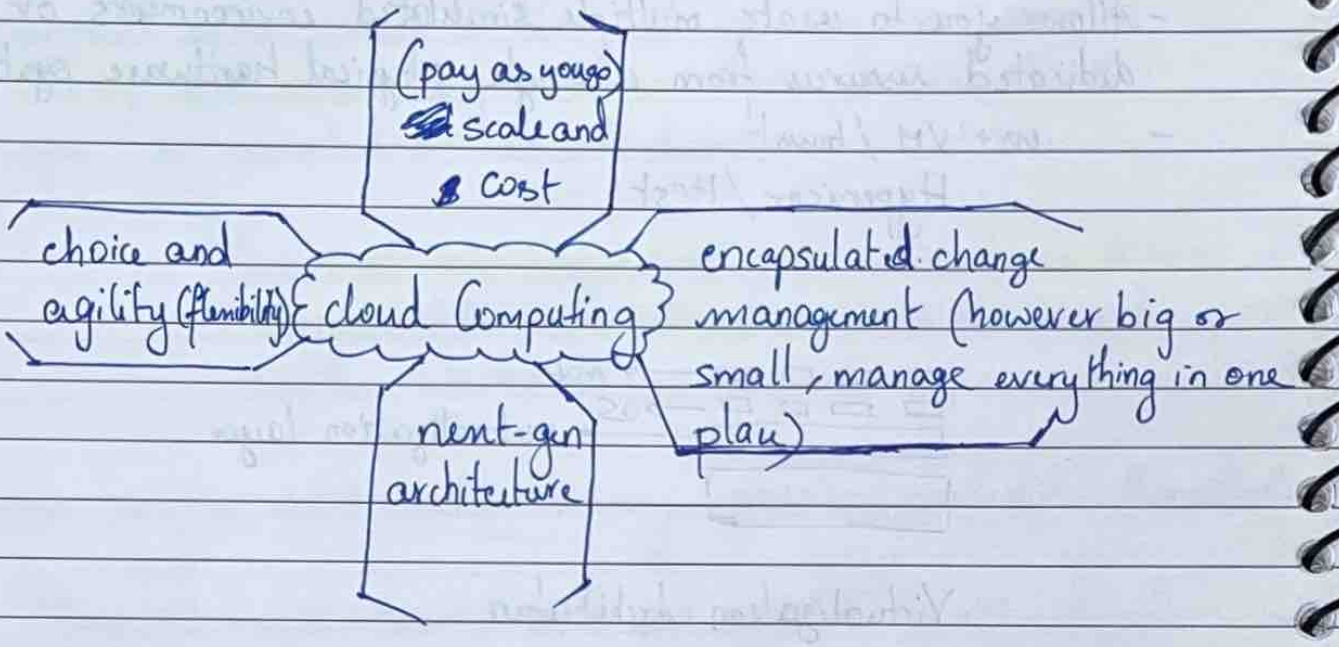
Optimize (resources are working for what you want)
③ Integrate → (business needs are integrated to cloud)
CLOUD
②
Manage → (once management is done, we move to cloud)
Automate → (services automated / items automated)
virtualize → (virtualize items in step 1)
① consolidate → (what needs to be moved to cloud)

M T W T F S S

Page No.: YOUVA

Date:

⇒ Cloud Computing



↳ Types : public (shared cloud) - tenant
: private (no shared resources)
: hybrid (private for sensitive assets and rest on public)

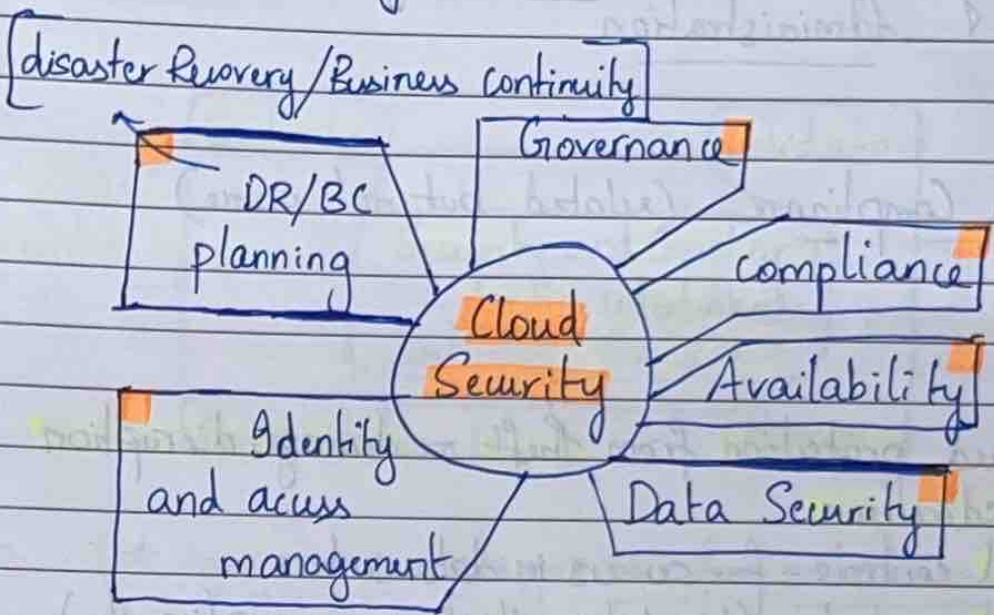
↳ moduls :

- SaaS (Software as a Service)
  - 3rd party hosting an application
- Paas (platform as a Service)
  - getting own platform to manage apps or tasks
- IaaS (Infrastructure as a Service)
  - delivers a whole computer infrastructure like storage servers, network devices, etc

↳ Benifits

- flexibility
- efficiency
- strategic value

Cloud Security



Cloud Governance

- Governance, Service and organigation should be aligned together.

- Governance - Service
  - portfolio mgt
  - service mgt
  - service integration
- Governance - organization
  - Team
  - function
- Cloud Strategy
- Service - Organization
  - prouss
  - Rols

reference model

- Cloud Consumer
- Cloud provider
- Cloud Auditor
- Cloud broker