data protection Cloud IAM

Date

Chapter 8 Intrusion Detection

Classes of Intruders

Cyber Criminals	Activists	State sponsored organisations	Others
Individuals with a goal of financial reward • Identity, data theft • financial credential Theft	Individuals or members of Larger group motivated by a social potical causes • DOS • Website defacement	• Conduct espionage or Sabotage activities • APTs	Hackers with other motivation

Intruder Skill levels

Apprentice : use existing tool kits
Journeyman : modify // //
Master : make tool kits

Examples of Intrusion

remote root compromise
web server defacement
cracking passwords

Intruder behavior

(a) Target Acquisition and information gathering
(b) Initial Access
(c) Privilege Escalation
(d) Information Gathering or system Exploit
(e) Maintaining Access
(f) Covering Tracks.

MAAZ

Date _____

Security intrusion: unauthorised act of bypassing the security mechanisms.

Intrusion detection: Hardware or software function that gathers and analyses information from various areas to identify intrusions.

Intrusion Detection Systems (IDS)

Host-based IDS	Network based IDS	Distributed or hybrid IDS
Monitors the characteristics of a single host for suspicious activity	Monitors network traffic, and analyses network transport and application protocols to identify suspicious activity.	Combines information from a number of sensors, often both host and network based in a central analyser.

Three logical components:
Sensors: collect data
analysers: detect
user interface: view

Analysis Approaches

Anomaly detection	Signature/heuristic detection (Rules)
• involves collection of data relating to the behavior of legitimate users over a period of time • Current observed behavior is analysed to determine whether this behavior is normal?	• uses set of known malicious data patterns that are compared with current. • AKA misuse detection • Only identifies known attacks.

MAAZ

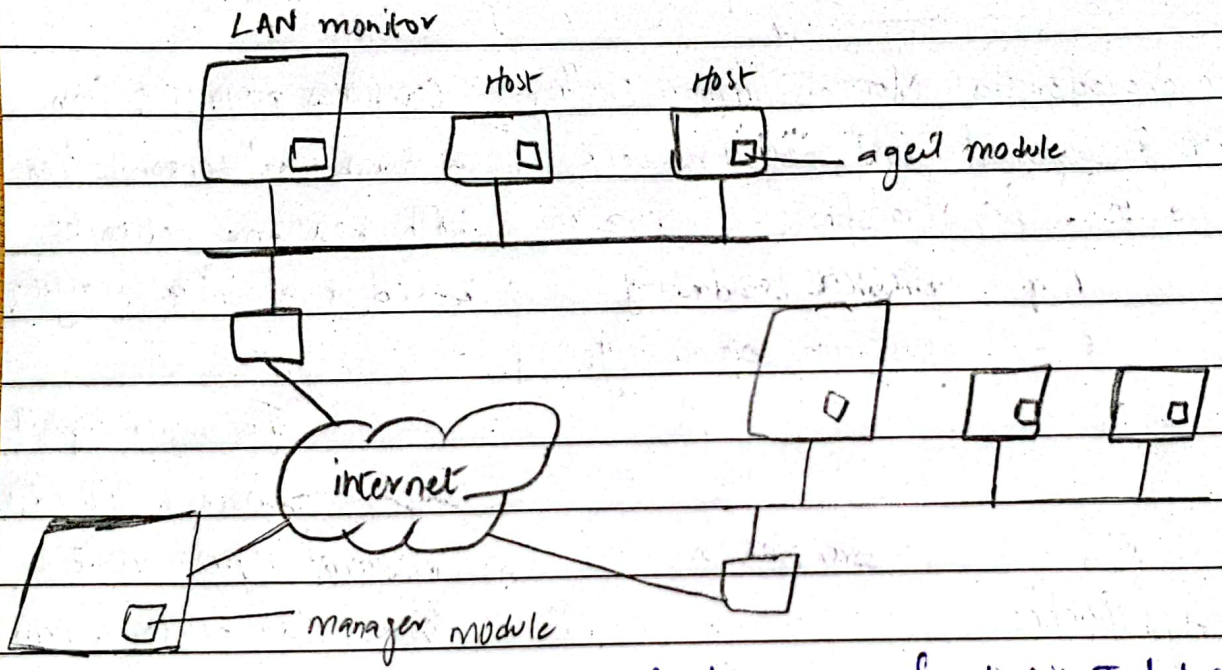
Date _____

Host-Based Intrusion Detection

- Can use either anomaly or signature and heuristic approaches
- Monitor activity to detect suspicious behavior and send alerts.

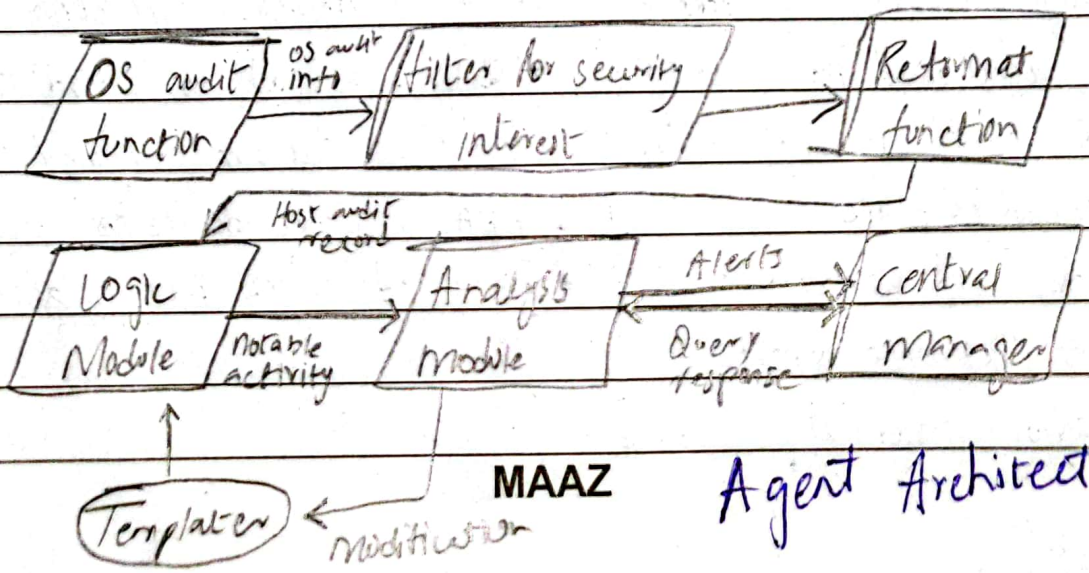
Sensors collect the data

data sources: system call traces, audit file, file integrity checksum, registry access



Architecture for distributed Intrusion Detection

central manger



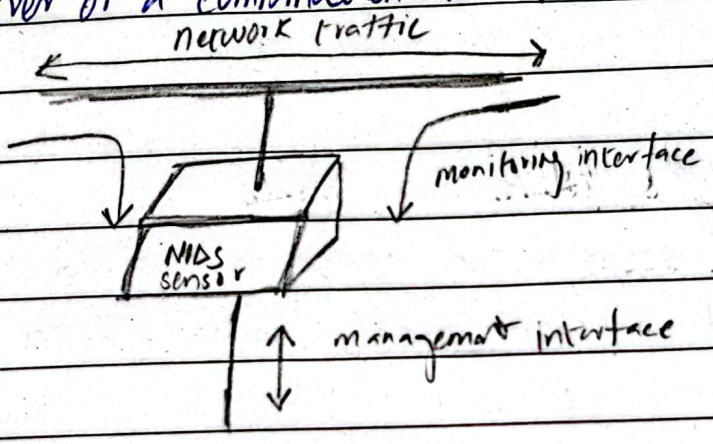
Agent Architecture

MAAZ

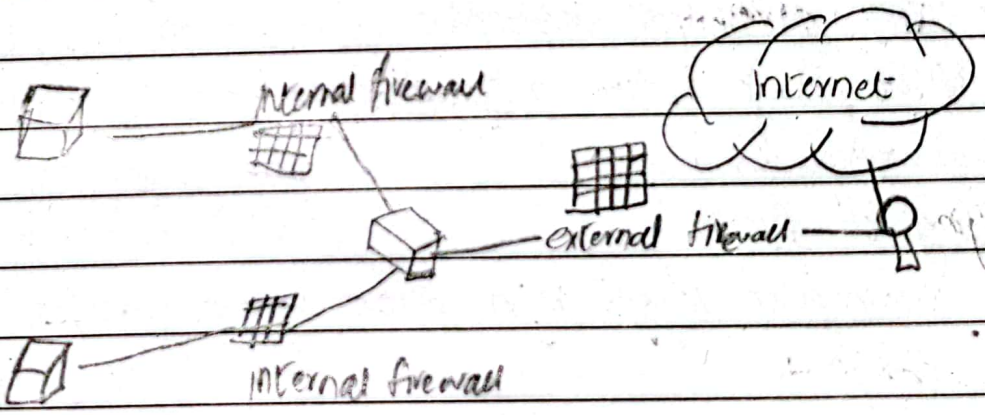
Date _____

Network-Based IDS

- Examines traffic packet by packet in real time
- Comprised of a number of sensors, one or more servers and management consoles for the human interface.
- Analysis of traffic patterns may be done by sensor, the management server or a combination the two.



Passive NIDS sensor



Date

Intrusion Detection Techniques

Signature Detection	Anomaly detection.
• Application layer reconnaise and attacks	DOS attacks
• Transport // // // //	Scanning.
• Network // // // //	worms.
• unexpected application services	
• policy violations	

Stateful Protocols Analysis (SPA)

- It is the subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles benign protocol traffic.
- Understands and tracks network, transport and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires.

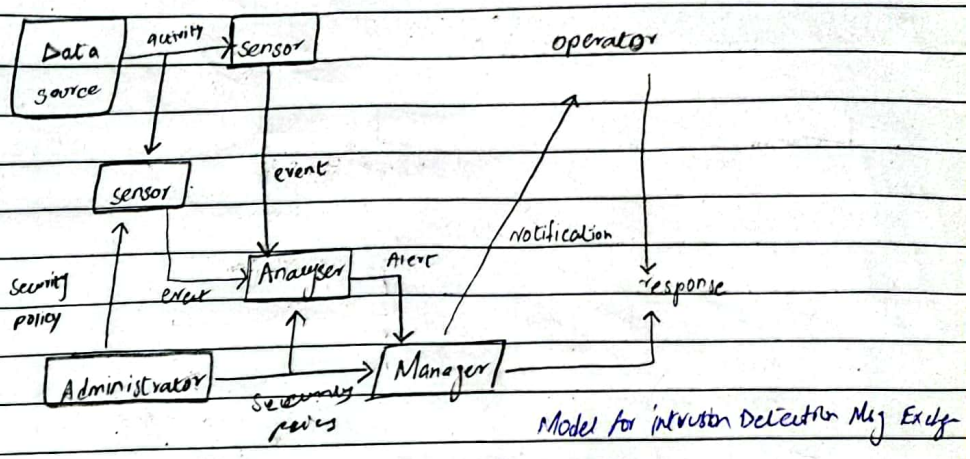
Logging of Alerts

Typical information logged by a NIDS sensor includes

- Timestamp
- Connection or Session ID
- Event or alert type
- Rating.
- Network, transport and application layer protocols
- Source and Destination IP address

MAAZ

Date



Model for intrusion Detection Mig Exdg

Honeypots

Decoy systems :- lure a potential attacker away from critical systems
- Collect info about the hacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

- They are systems filled with fabricated information that legitimate user of the system wouldn't access.
- Resources that have no production value (incoming communication is probably a scan)

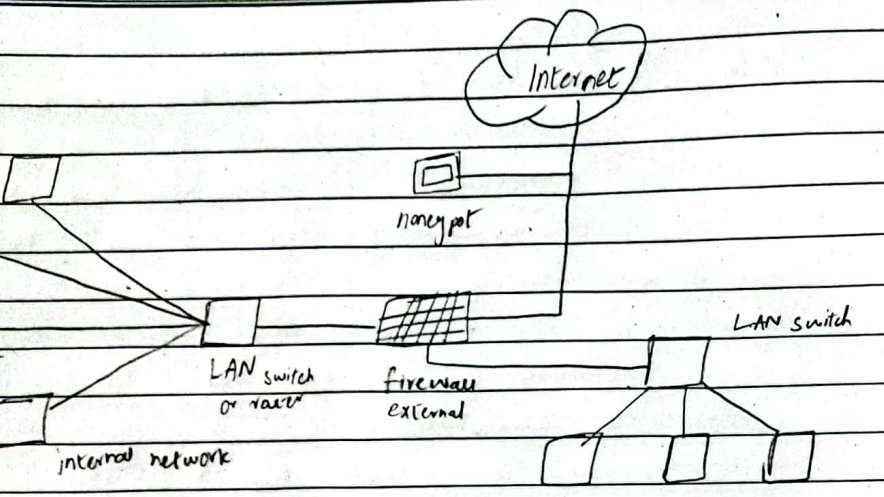
Honeypot classification.

low interaction Hp : emulates particular IT services or systems well enough to provide a realistic initial interaction but does not provide full version.

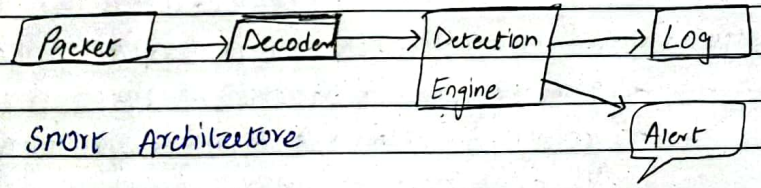
High interaction Hp : A real system, with a full operating system, services, requires more resources, if compromised could be used to initiate attacks on other systems.

MAAZ

Date _____



Example of honeypot Deployment



Snort Architecture

Date _____

Chap # 9 Firewalls and Intrusion prevention Systems

Need for Firewalls

- effective means of protective LANs.
- Used as a parameter defense.
  - single choke point to impose security
- Inserted between premise network and internet.

Characteristics of firewall

- All traffic must pass Through the firewall
- Only authorised will pass Through as decided by local security policy
- Firewall itself is immune to penetration

Firewall Access policy.

- Types of authorised traffic to pass through e.g address ranges, protocols and Apps.
- policy should be developed from organisation's security and risk assessment policy

Firewall filter characteristics

IP address / protocol value	Application protocol	User identity	Network Activity
• packet filtering • stateful inspection firewalls.	Application level gateway That relays and monitor exchange of info for Specific Application protocols.	inside users who identify Themselves using Authentication	Controls Access based on time, request or Activity patterns.

Date

Firewall capabilities and limits.

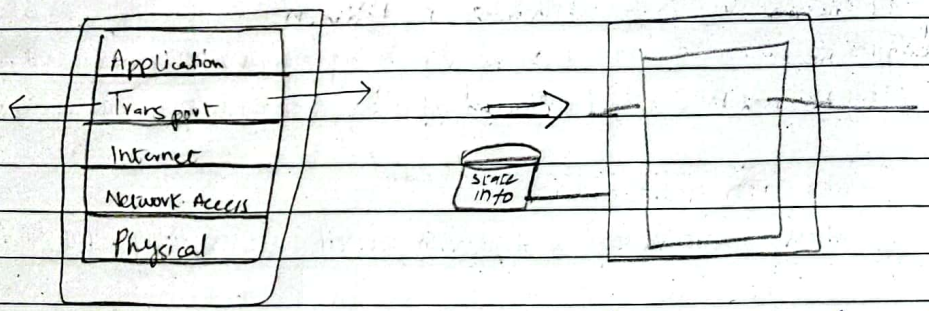
Cap

- defines a single choke point.
- provides a location for monitoring security events.
- Convenient platform even for functions not security related

Limitations

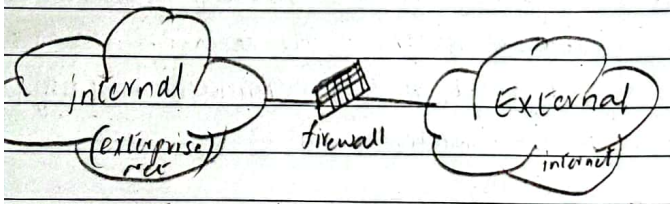
- Cannot protect against attacks bypassing firewall.
- May not fully protect against internal threats.
- Devices or may be infected if outside the corporate network.

Types of firewalls.



Packet filtering

Stateful inspection firewall

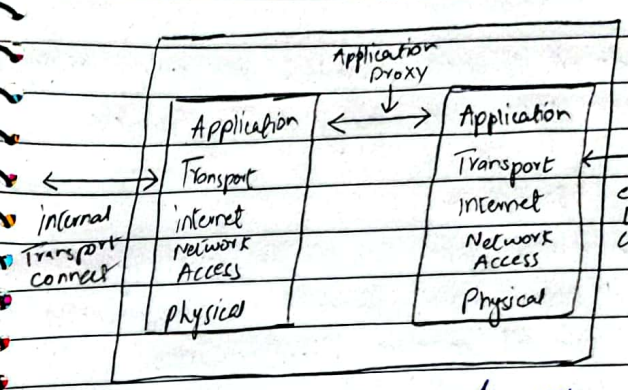


protected

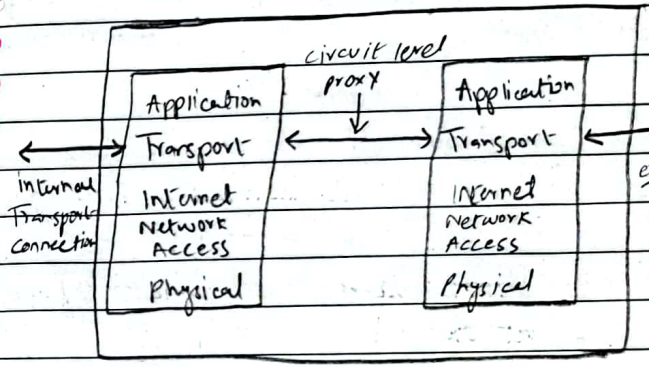
General model

MAAZ unvisited

Date



Application proxy firewall



Circuit-level proxy firewall.

Packet filtering firewall.

Applies rules to each incoming and outgoing IP packet

It forwards or discards the packet based on rules match.

Rules :- Source, dest IP address

- source / dest transport level address
- IP protocol field.

TCP (ACK) is used to secure

MAAZ

Date

Most packet filter firewalls do not support advanced user authentication schemes. due to the lack of upper layer functionality by the firewall

Adv	Disadv
• simplicity and transparency to users	• Cannot prevent attacks exploiting Application-specific vulnerabilities
• Fast operation	• Limited logging functionalities.
	• lacks support for advanced user authentication
	• Vulnerable to attacks on TCP/IP • improper config leads to breach

Common Attacks on Packet filtering

IP address spoofing: Attackers use a fake IP address. (internal)
Counter Measure: Discard packets with an inside source address on external interface

Source routing attacks: Attackers specify the route a packet should take to bypass security
Counter Measure: Discard packets that use source routing.

Tiny fragments attacks: Attackers create tiny fragments to bypass ~~security~~ filtering rules
Counter measure: first fragment must contain some transport header else all rejected

Problem: A traditional packet filter allows incoming traffic on all the temporary doors (high numbered ports). This openess can be exploited by unauthorised users.

Date

Stateful Packet Inspection firewall: SPI

SPI firewall keeps a directory of all the active communication channels (TCP)

Selective access: The firewall now only allows incoming traffic on high numbered doors if it matches the ongoing conversations listed in the directory others are blocked

Preventing Specific Attacks: Keeps track of TCP ~~connections~~ sequence numbers to prevent attacks that depend on the sequence number. And inspects data for protocols like FTP, IM, SIPS

Application Level Gateway

AKA application proxy. It acts as a relay of application-level traffic
- User contacts gateway using TCP/IP application.
- User is authenticated
- Gateway contacts application on remote host and relays TCP segments between server and user

Adv: more secure than packet filter
DisAdv: processing overhead and slower processing.

Date

Circuit level gateway

- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host.
- Relays TCP segments from one connection to the other without examing contents.
- Security functions consist of determining which connections will be allowed
  - used when inside users are trusted

Socks clg

When (a program inside network) to talk outside, it talks to sock server first
Server and program negotiates, how to prove identity of the person inside

Intrusion Prevention System (IPS)

A system with capability to attempt to block or prevent detected malicious activity
It can be host, Network based or distributed / hybrid
It not only spots threats but also tries to stop them.
Can use anomaly and signature / heuristic detection

Host-based IPS (HIPS)

It can use anomaly and signature/ heuristic detection to identify attacks behaviors addressed by HIPS.

- modification of system resources : stop changing from computer parts.
- Unauthorised access : blocks to get high level access
- Email Safety :
- folder exploring :
- Memory exploits : mess with memory to get sneaky attacks

MAAZ

Date

HIPS work

Tailored protection : tailored to specific platform
Special tools : special tools for special files.
Sand box Approach : tries out runs suspicious stuff in safe area before in computer
Desktop protection Areas : protections for
system calls.
file system access

Network-based IPS (NIPS)

- NIPS with authority to modify or discard packets and tear down TCP connections.
- uses anomaly and signature/heuristic detection.
- Methods use to identify
  - Pattern Matching :
  - Stateful // : scans for attk signature in context of a traffic stream than indiv
  - Protocol anomaly : looks for deviation from standards set in RFCs
  - Traffic // : watches unusual traffic such as trad new service
  - Statistical // : Develops baseline for normal traffic and alert if deviation.

Distributed or hybrid IPS

Gather data from a large number of host and network based sensors, relays this intelligence to a central analysis system which identifies patterns and learns new threat and updates all the guards with info making smarter e.g digital immune syste

MAAZ

Date

Digital immune system

Developed by IBM due to rising threat level and speed of propagation

Snort inline

IPS - Snort inline is more than just an alarm, it actively prevents potential threats

Replace option - instead of stopping / dropping a suspicious packet it modifies the content of packet before letting it in.

Useful for honeypots - Snort inline make it look like it worked (fail silently) confusing attacker as they're attack is not impacting

Drop, Reject and Sdrop =

Drop - snort rejects a packet based on rules and logs the action

Reject - similar to drop but sends an error msg to the sender

Sdrop - similar to drop but doesn't log the action useful when not to leave a trace of every rejected packet

MAAZ

Date

Chap 14 IT security Management and Risk Assessment.

Ensure critical assets are sufficiently protected in a cost effective manner

IT security management functions include

Determine organisation's IT security objective, strategies, policies // // // requirements

Identifying and analyzing risks.

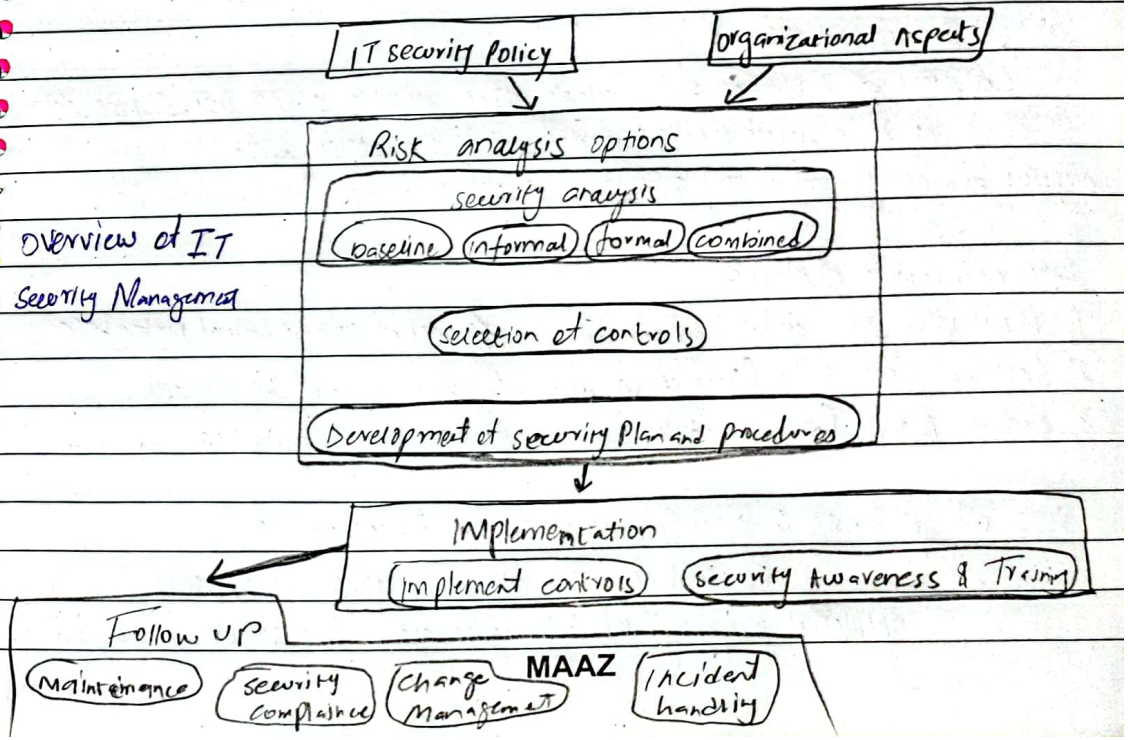
Specifying appropriate safeguards.

Monitoring and implementing of safeguards

// ↑ security awareness program

Detecting and reacting to incidents

Overview of IT Security Management



MAAZ

Date

Approaches to identify and mitigate risks

Baseline : Protection against most common threats
using industry best practices
recommended only for small organizations with resources

Informal : conducts pragmatic risk analysis on organization's IT systems
Judgements made about vulnerabilities and risks
Suitable for medium sized orgs when IT system not essential

Chapter 19 legal and Ethics Aspects

Types of computer crime :
Computers as a target : Criminals attack computer to gain info, disrupt data
Computers as a storage device : Computers to store stolen data.
Computers as a communication tool : Traditional online crimes fraud, illegal sales.

Law enforcement challenges :
1) Investigative difficulty (lack technology)
2) Resource Constraints (lack computing power)
3) Global Nature (other jurisdictions)
4) Lack of Cyber Criminal Database
5) wide range of behaviors
6) Low Reporting Rates

Types of property : Real Property : Land and structures
Personal Property : moveable items, cars, money.
Intellectual property (IP) : Intangible assets like software, data, ideas.

MAAZ

Date

Intellectual property Types :
1) Copyrights : Protect tangible assets e.g books, music and software
rights = Reproduction, modification, distribution.
2) Patent : Grant property right for invention eg design, utility
3) Trademarks : Identifying the source of goods and services e.g logo, brand name

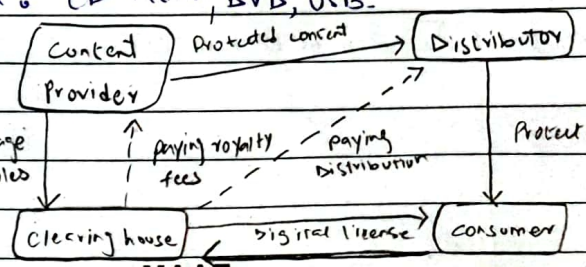
As of computer Securing copyright of software, DB, digital content and algo of org should be done

Protection Measures : Technical security : computer security safeguard of data/info
legal protection : copyrights and patents

Digital Millennium Copyright Act (DMCA) : Protects digital content rights Globally
Exemption : fair use, reverse engineering, encryption research, security testing and personal privacy.

Digital Rights Management (DRM) : ensuring creators are identified and paid for digital work
Functions :
Persistent content protection : Limiting access to only authorised ppl.
Support variety of digital content : music, video, book, image.
" " use on platforms : computer mobile tablets
" Content distribution : CD ROM, DVD, USB.

DMCA : Protects digital content
DRM : Ensure created get paid usage Rules



DRM Component

MAAZ

Date _____

Privacy Law and Regulation Principles

- Notity — Access — enforcement
- Consent — Security
- Consistency — Onward transfer

Computer Usage privacy

Anonymity : User use resource without revealing identity

Pseudonymity : // // // // // but can be accountable

Unlinkability : Other can not link Them.

Unobservability : Third perties cant observe

Addressing privacy concerns

Technical approach

- Db security
- Privacy setting
- Anonymizing data

Policy Approach

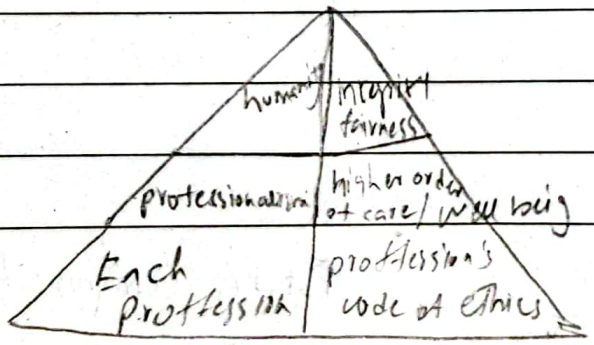
1. consent
2. Privacy / confidentiality
3. ownership (4) governance and custodian
5) Data sharing (reuse of data)

Ethics in IT professions : Ethic involve moral principles related to actions and their consequences

Ethical Decimas for Professiels : Whistle blowing, employees conflict of professand loyalty to expose Formdy And potential conflict of interest

Codes of conduct : Function of code of conduct : Inspiration, image educational, supportive

deterant : means of consequences



MAAZ

Date _____

Ethics is moral compass

Ethics : A system of moral principles that relates to the benefits and harms of particular actions and to the rightness and wrongness of motives and ends of those actions

Ethical issue from computer issue :-

Repositories and processors of information: unauthorised use of unused computer or of info stored in computer

Producers of new forms and types of assets:

Instruments of acts : Computers are tools that people use to perform

Symbols of intimidation and deception:

Social power : ability to influence or control things in society but in a way that follows the accepted rules

Rules :

Creator's responsibility

Not a Crime

User's responsibility

Think about the system

No Deception

MAAZ