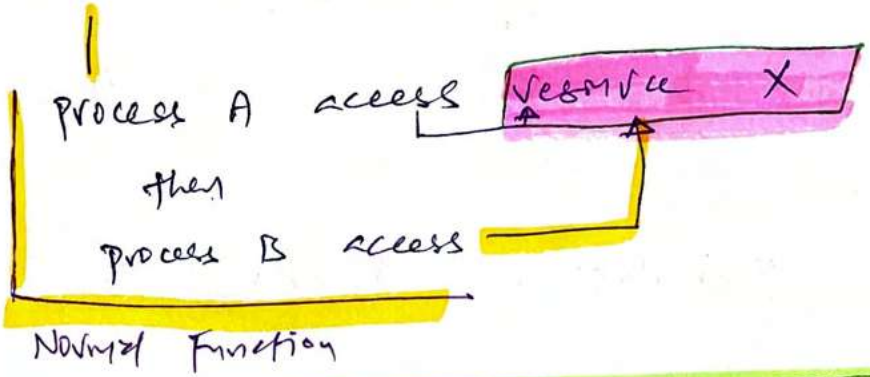
Race conditions – Two or more process need to access same resource in right order.



Split Knowledge

- Requires something you know
- E.g password is "SkyisBluefor46"

Person 1 → Skyis
person 2 → Blue
person 3 → for
person 4 → 46

- Split knowledge is logical

Dual control

- Requires something you do
- E.g. President + Secretary of defense + General turn their key to launch nuclear missile
- Dual control is physical

Split knowledge and Dual control similarity :-
Both holds two or more people responsible for one critical function.

Common Access Control Attacks

1. Access Aggregation Attack

collect non-sensitive information → to learn sensitive information

E.g → Reconnaissance Attack

Prevention → Least privilege, Need-to-know & Defense-in-depth

2. Password Attacks

P.T.O end

--- Hybrid Attack first use dictionary then it use Brute-force.

P.T.O

Dictionary Attack

- Use of predefined passwords from Database

Brute-Force Attacks

- Attempt to discover password using all possible combination of letters, numbers & symbols.

possible key values

Prevention → Use longer password with uppercase / lowercase / numbers & symbols

Birthday Attacks

- Focuses on finding collisions.
- This method doesn't need all possible hashes to see a match.

Prevention - Don't use MD5
Use SHA-3 with enough bits
SHA-3 with 512 bits.

All password cracking tool does is to find matching hash value of guess password. Hashing being a one way function, it's impossible then two hashing value but MD5 is not collision free. Remember that collision means it can match the hash.

Rainbow table

Why waste time guessing passwords & matching / calculating hash values when Rainbow table reduces this time by using large database of precomputed hashes.

Prevention → Use Salt to reduce rainbow attack

Random bits added to password before hashing it.

Password-Based Key Derivation Function 2

Bcrypt & PBKDF2 are common algorithm to salt passwords

Further prevention → Add Pepper

- If attacker gets the database, they also gets salts for the password
- Pepper is large constant number stored elsewhere

3. Sniffer Attacks

- Snooping or Eavesdropping Attack

Prevention

- IDS
- Use one time passwords
- Protect N/W device with physical security
- Encrypt all sensitive Data

4. Spoofing Attacks

- phone spoofing.
- IP Spoofing
- Email spoofing

Prevention

- Don't click on suspicious email / link
- Don't open unexpected email attachment
- Be careful from unknown senders

Phishing Attack

- Trick users to give up their sensitive information
- E.g Email with link

Drive-By Download

- Type of malware that installs itself without user's knowledge when user visits the website. it traces advantage of vulnerabilities in Browser / plugins.

5. Phishing

Spear

- Target to specific group of users, employees within a specific organization.

Whaling

- Targets senior / high-level executives (CFO), president of company

Vishing

- Use of phone / VoIP
- commonly spoof caller ID to impersonate Bank / financial institutions.

6. Social Engineering Attacks

Shoulder surfing

7. Smart Card Attacks

Side channel Attack

- Passive Attack where Attacker learn valuable info. contained within card such as Encryption key.

DOMAIN 6

CH: 15 SECURITY ASSESSMENT & TESTING.

So far,

Build and Implement security controls

This chapter,

Regularly test security controls and ensure they are working properly, and effectively safeguarding information assets.

COMPONENTS OF Security Assessment Program

1. Security Test
2. Security Assessment
3. Security Audits

P.T.O

Is security control functioning properly?

- configuration drift
  - check operational evidence
    - ↳ Automated Scans
    - ↳ Tool assisted Pen tests
    - ↳ Manual attempts

Risk assessment / Exposures

NIST 800-53A

Four components of Assessment

P.t.o

NIST 800-53A

1. **SPECIFICATIONS:** Docs associated with audit
   - Procedures
   - Policies
   - Requirements
   - Specifications

2. **MECHANISMS:** These are controls within Information system & to meet specifications.
   - Based on - hardware
     - software

3. **ACTIVITIES:** Action carried out by People within Information System.
   - Perform Backup
   - Log export
   - Review AC histories

4. **INDIVIDUALS:** People who implement
   - specifications
   - Mechanisms
   - Activities

Audit is different from Assessment & Testing

internal use only

To show buyer/3rd party that security doors are installed with triple lock.

House is clean from inside. security doors/windows are working for internal protection.

Auditors = Unbiased view

SECURITY CONTROL

Internal Assessment & Testing = likely biased

3 Types of AUDITS

INTERNAL

- Internal Audit staff for internal Audience
- These audits normally have a reporting line that is completely independent of functions they evaluate.

EXTERNAL

- Auditing firms
- Has no conflict of interest with organization.

THIRD-PARTY

Third-party Audits

- Conducted by / on behalf of other organization

↓

Burden if large number of client

→ AICPA released **SSAE 16**

(Statement on standard for Attestation Engagement Document 16)

Provides one common standard for auditing

Type I report SOC

- Description of control + opinion of auditor based on control description
- No actual testing of control (-VE)
- Controls are implemented as they described

RELIABLE Type II report SOC

- Covers min. 6 months + opinion of auditor on effectiveness of the control
- Actual testing of control by Auditor (+VE)

AUDITING STANDARDS

- **COBIT** – Control objectives for Info. & related technologies
- **ISO 27001**
- **ISO 27002**

ISO – International organization for Standardization

PERFORMING VULNERABILITY ASSESSMENTS

Actually, it's vulnerability testing tools, not vul. assessment tools.

Vulnerability Scanning + Pen Test → To find weakness in System / Applications technical controls.

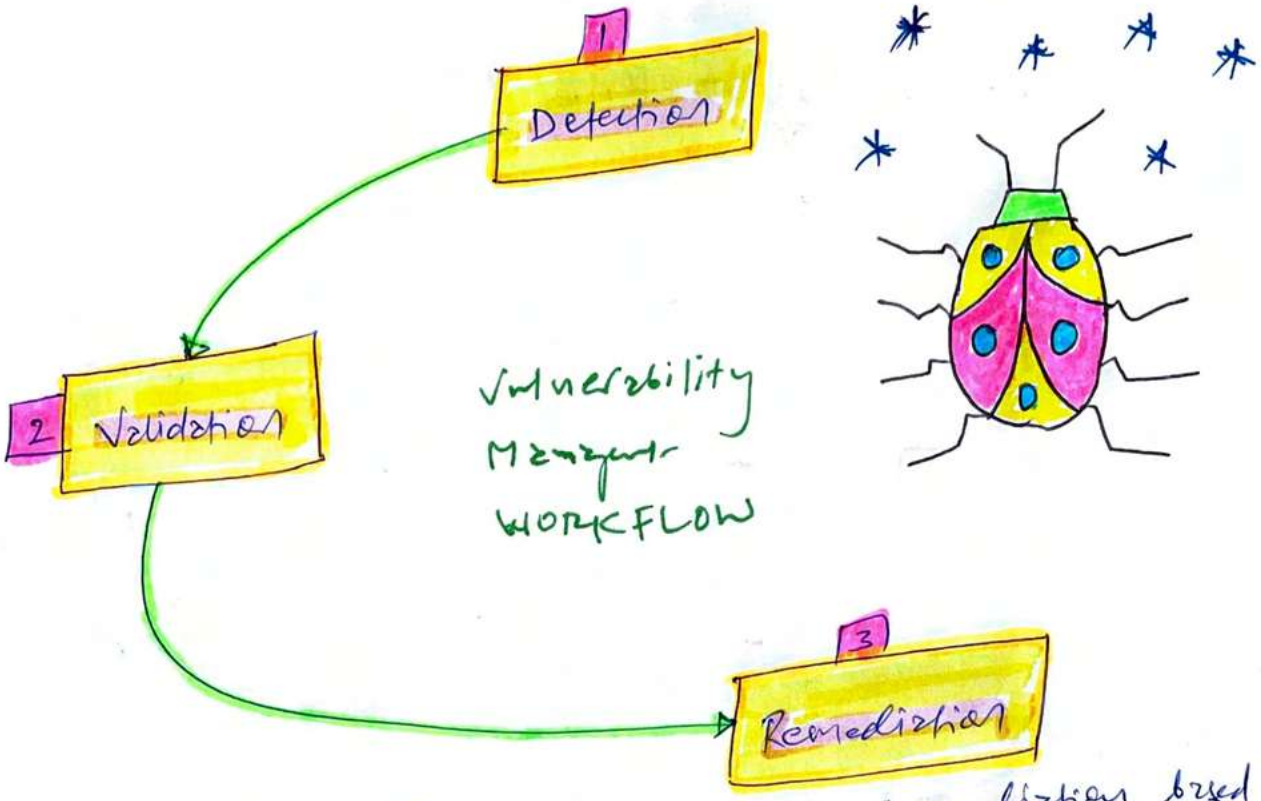
1. Network Discovery Scans
   - opens half-connection → TCP SYN scanning
   - opens full-connection → TCP connect scanning
   - TCP ACK scanning
   - Xmas scanning.

   (NESSUS, Rapid7) NMAP

2. Network Vulnerability Scanning.
   - Scan open port + find known vuls.
   - False negative is dangerous than False positive
   - To Reduce → To perform authenticated scans over unauthenticated scan

3. Web Vulnerability Scanning
   - Similar scan to N/w vul. but scan more on web application structure.
   - Web App scan may require for compliance such as PCIDSS.

4. Database Vulnerability Scanning
   - sqlmap: open source tool to detect vuls.
   - Database security issues (ch:9)



Prioritize vulnerability remediation based on:

- Severity of the vulnerability
- Likelihood of the exploitation
- Difficulty of remediation

REMEMBER AGAIN

Security vulnerability assessment is NOT about assessment, but it's about

Security testing.

Penetration Testing

Phases

Planning → Testing scope is crucial. UI + backend

Info. Gathering & Discovery ← Perform Reconnaissance → Automated / manual tools to collect info. about target system or environment. E.g. nmap for n/w discovery.

Vulnerability scanning → Database vul. scan; Web vul. scan; Network vul. scan

Exploitation → Kali Tools.; Metasploit tool: for common attacks. Automatic exploitation on target system.

Reporting → Summary of test + recommendation; Raise risk

Ethical hacker use only this type of pen test method

4. Double Blind

3 Kinds of Pen Test

1. Whitebox Pen Test

- Provide full targeted system to Attacker
- short time
- likelihood to find security flaws.

2. Gray Box Pen Test (Hybrid)

- Balanced / Hybrid / Partial knowledge test
- Use when you want Black Box test but have no time & money

3. Blackbox Pen Test (Si

- Doesn't provide any info to Attackers
- more time + money $$$
- Simulates genuine external attack

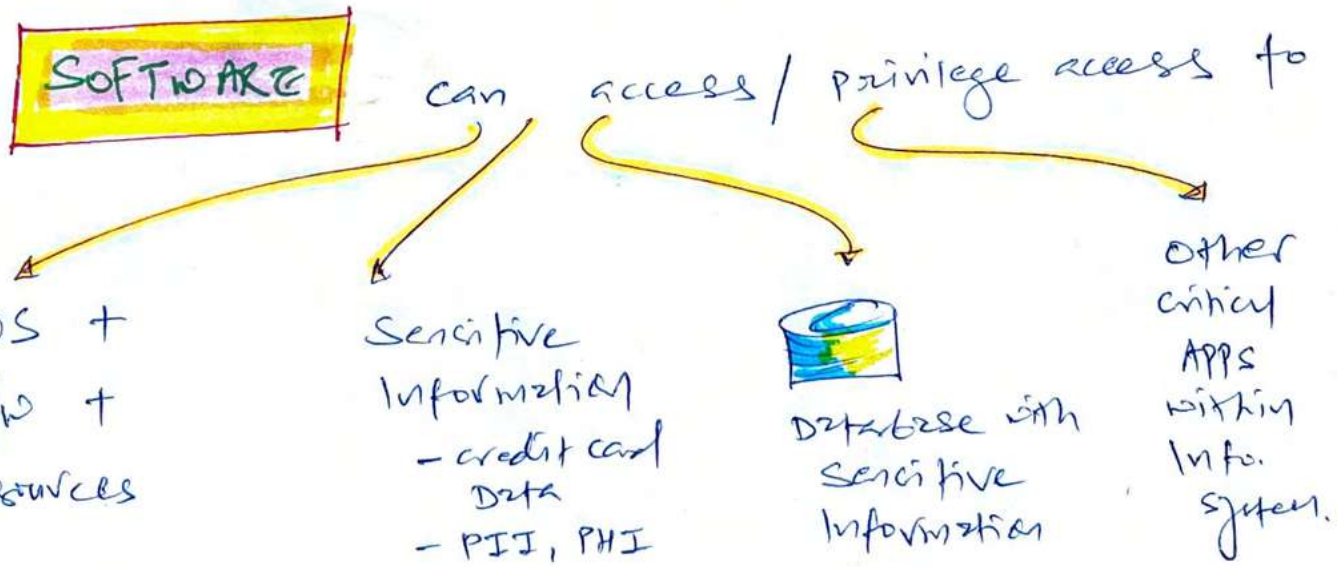
Industry standard Pentest methodologies

- OWASP testing guide (Application security)
- PCI DSS Information Supplement (Financial Data Security).

so far.....

SOFTWARE TESTING.

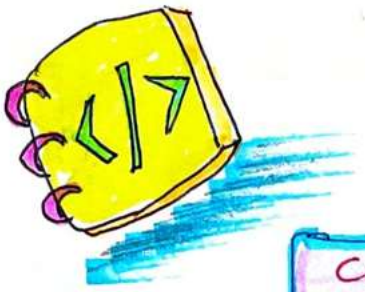
why take software seriously ?
or
why software is the heart of modern enterprise



Software testing → Essential to CIA requirement of modern Organization

SDLC / ch: 20.

Critical components of software testing



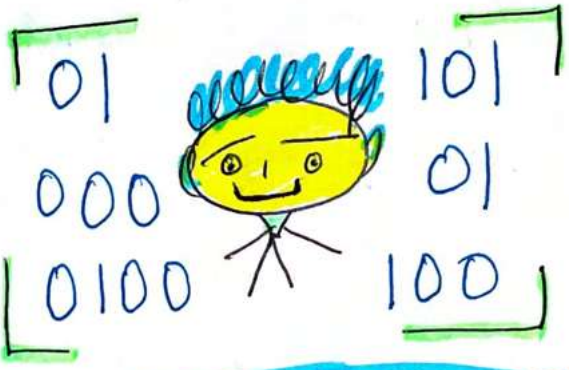
Code Review

FAGAN = most rigid code review process

1. Planning
2. Overview
3. Preparation
4. Inspection
5. Rework
6. Follow-up

Testing

- static (SAST)
- Dynamic (DAST)
- Fuzz
- Interface
- misuse case
- website monitoring



Human can do below types of code review

- software inspections
- software walkthrough
- Code Review

But not this

- Static program Analysis as it's done by Automated Tools

Static testing

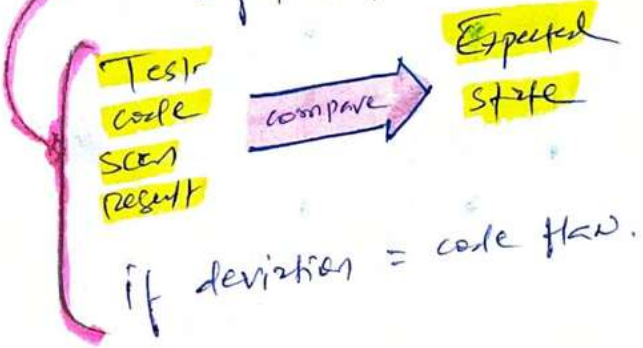
- Evaluates software security without running software. Instead, it analyze / scan source code.

- SAST: We can use this during Pre. prod (Design, build & test) of CI/CD pipeline

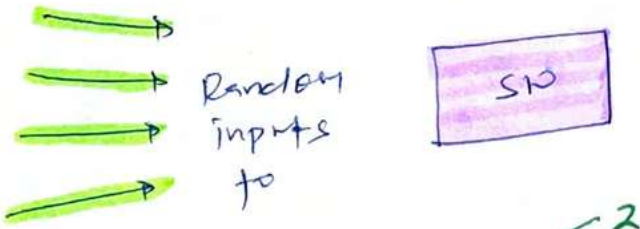
Dynamic Testing

- Not focused on / scan source code as apps / s/w is deployed in prod / runtime environment.

- May include synthetic transactions. to verify system performance.



Fuzz Testing ← Black box testing



= s/w crash, buffer overflow, undetected flaws.

2 types

Dumb Fuzzing (Mutation)

- Fuzz tool manipulates input (bit flipping) to confuse s/w (osh page 684-685)

Intelligent Fuzzing (Generational)

- Develop data models to create fuzz input based on the understanding of types of Data.

Interface testing

3 types of Interface to test during s/w testing :

- Application Programming Interface (API)
- User Interface (UI)
- Physical Interface

Internet

User clicks, Data requests, Login, Url

Website monitoring

Passive

- Real-time live traffic for real user interaction
- Detect issues for real user after it occurs
- Tool: Real User monitoring (RUM)

Synthetic / Active

- Initiate artificial transaction with website to check performance
- Can't detect real user issues but we can detect issues before it actually occurs.

Minority reports

- Variant of passive monitoring, it records users interactions with App / website to ensure quality and performance

Misuse case Testing

s/w developer use → - Abuse case testing to evaluate vulnerability of s/w to known risks

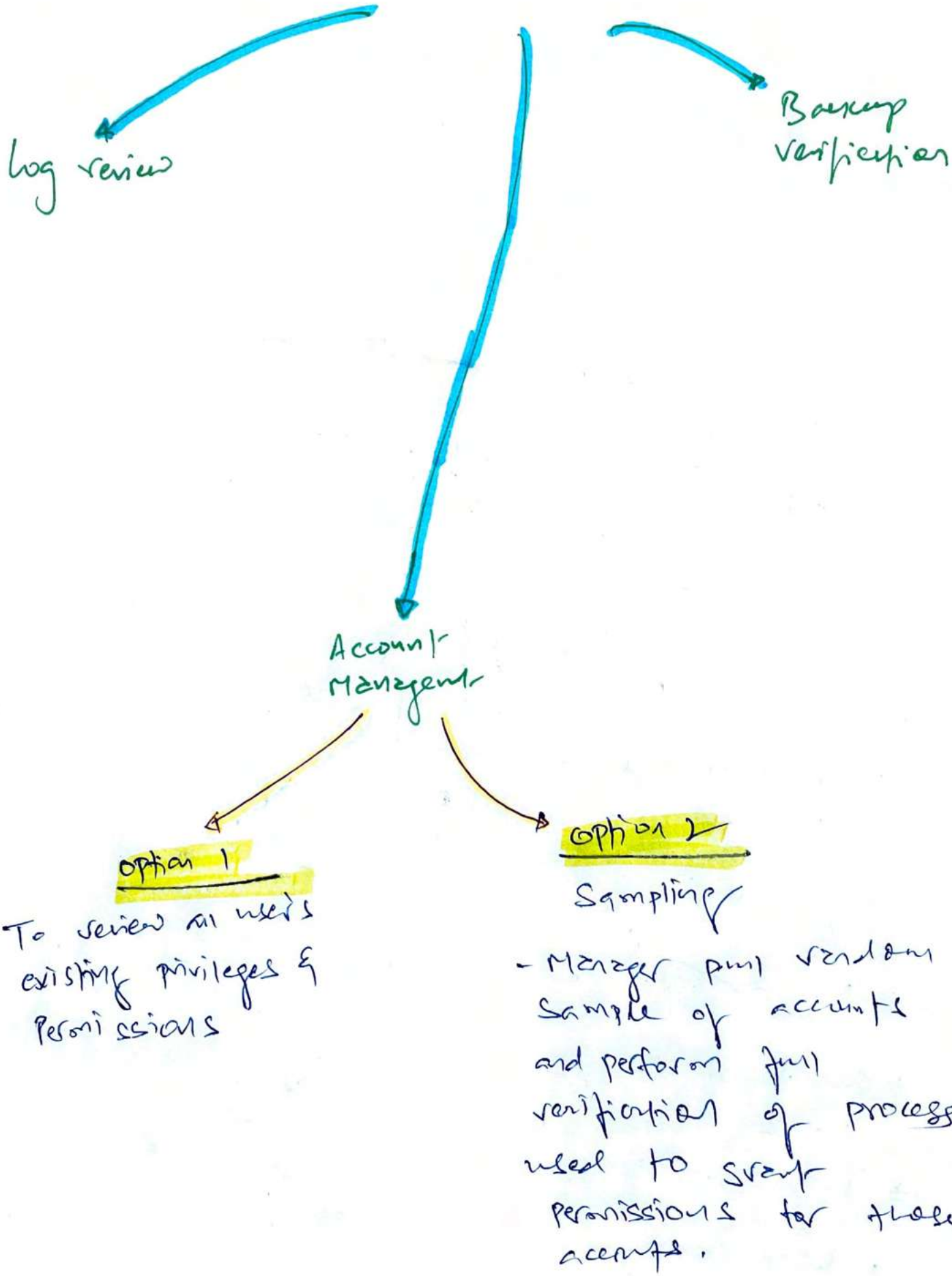
Test coverage Analysis — For new softwares

s/w testing professional use below formula for new s/w

$$\text{test coverage} = \frac{\text{no. of use cases tested}}{\text{total no. of use cases}}$$

- Branch coverage - if/else conditions
- conditional coverage - logical test in the code
- Functional coverage
- Loop coverage - conditions that cause code execution multiple times
- Statement coverage - test every line of code

Implementing Security Management Process



Post Q&A - wrong answer topics

* Describing Vulnerabilities

NIST provides SCAP (Security content Automation Protocol)

A framework to describe common vulnerabilities.

Components of SCAP

CVE
- Common Vul. & Exposure
- Identifies vul. generated by diff. security Assessment Tools
- consistent naming system/ reference to identify vul.

CCE
- Common config. Enumeration
- Naming system for system configuration issues.

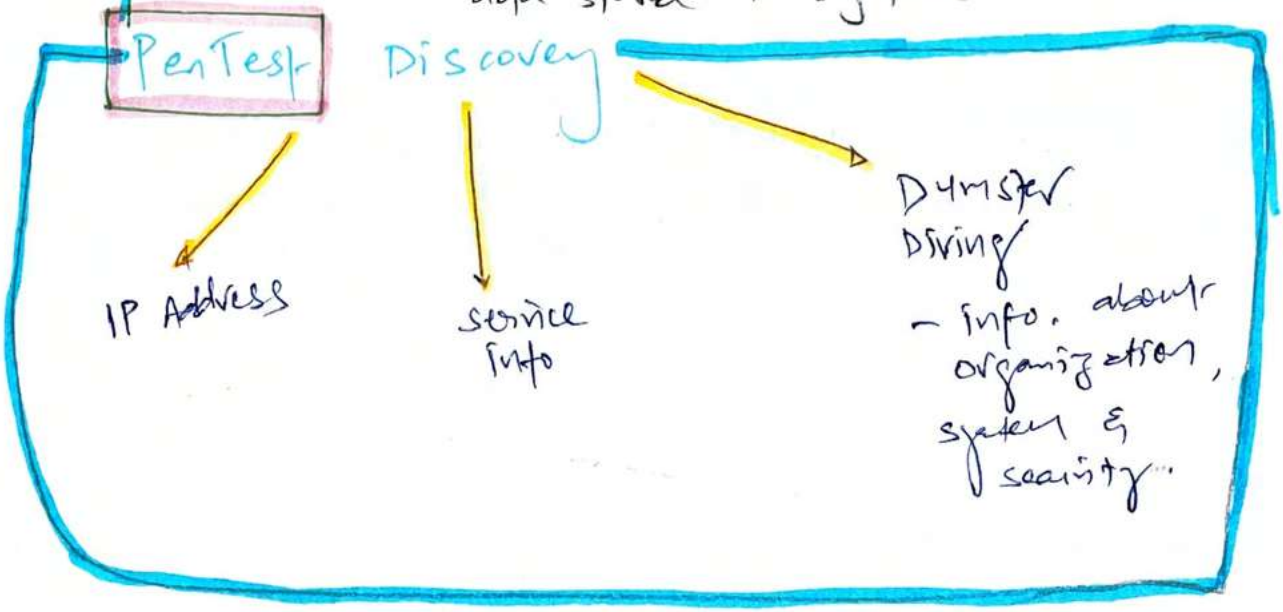
CPE
- Common platform Enumeration
- Naming system to refer consistent name for operating system

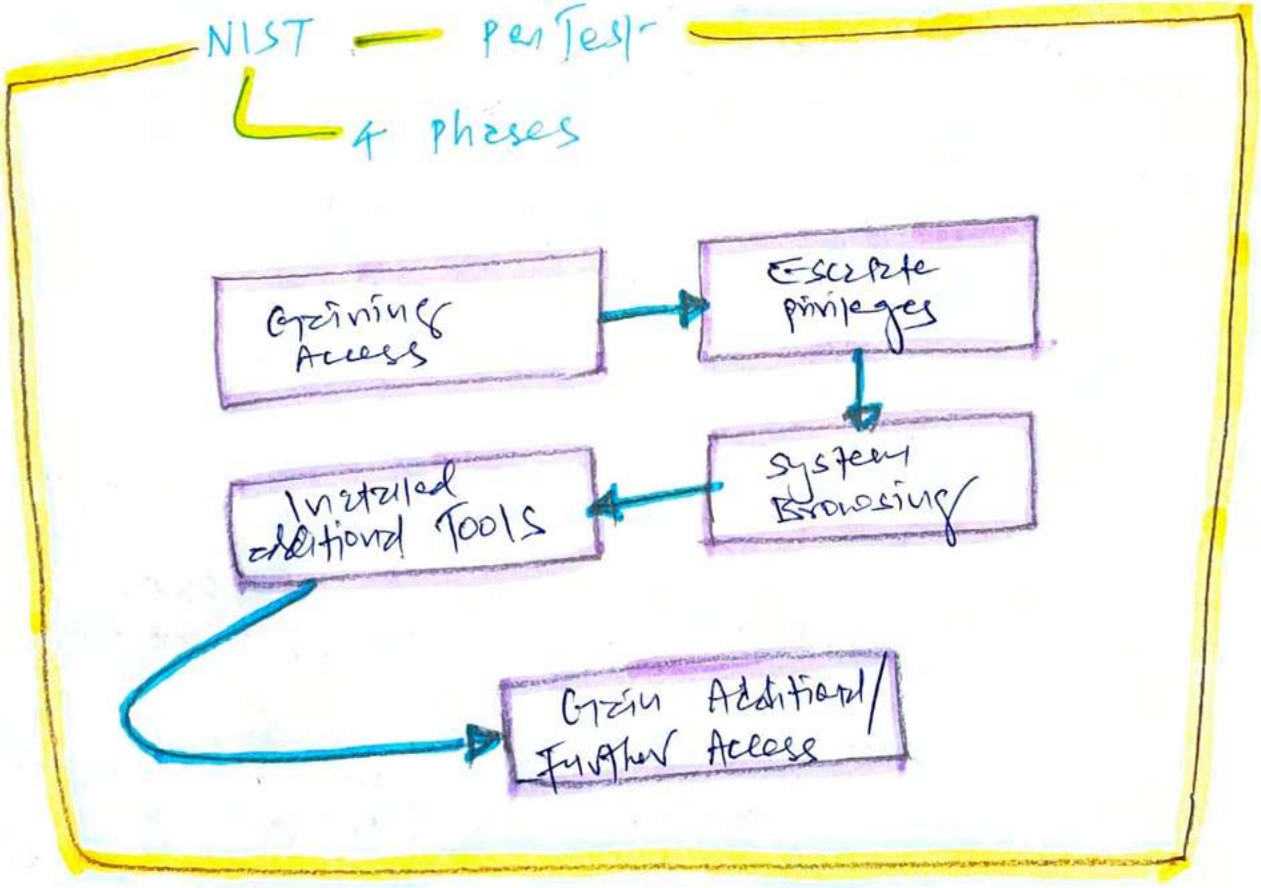
CVSS
- common vul. scoring system
- Describes severity of security vul.

OVAL
- open vul. & Assess. language
- Describes security condition of system
- Provides language for describing security testing procedure.

XCCDF
- Extensible configuration checklist Description Format
- Provides language for specifying security checklist

Hazard: May disrupt system access or corrupt data stored in systems.





PenTest report doesn't have sensitive Data. it has list of vuls, mitigation guide & risk rating.

Port
- is open, no access to App — closed
- is open, access to App — Open
- not accessible — Filtered (could be firewall)
  (Port could be open or close)

Reports
- Test coverage Report
  - how many test cases have been completed
  - Provides metric when uses test cases
- PenTest Report
  - upon conducting PenTest
- Line coverage Report
- code coverage Report
  - How much code has been tested

kind of

Coding issues → Bound checking, Input validation, pointer manipulation

Environment issue → Race condition
- code testing in manpred & prod arise in fixing issue

Unlikely to find in web vulnerability scanner

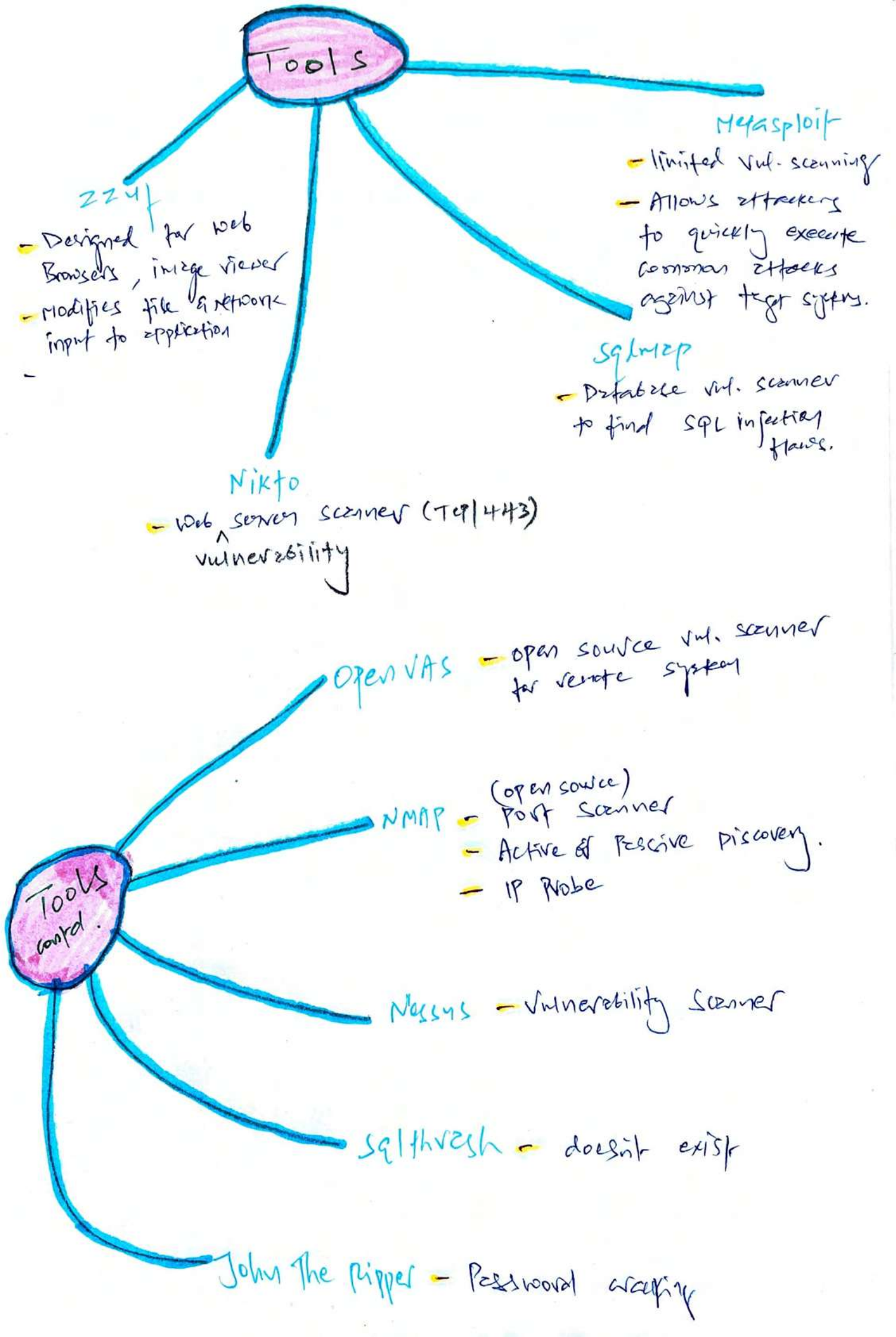
s/w Testing

Static → Analyze source code without running software

Dynamic → NO source code, for runtime
- Synthetic transactions to verify system performance

Fuzz → Mutation (Dumb)
- modifies program in a small way
- takes input from valid operations manipulates to create fuzzed input

Generational (Intelligent) — 224+ tool
- Develops data models & creates fuzz inputs


Tools
ZZUF
- Designed for web Browsers, image viewer
- Modifies file & network input to application
Metasploit
- limited vul. scanning
- Allows attackers to quickly execute common attacks against target systems.
sqlmap
- Database vul. scanner to find SQL injection flaws.
Nikto
- Web server scanner (TCP/443) vulnerability
Tools contd.
OpenVAS - open source vul. scanner for remote systems
NMAP (open source)
- Port Scanner
- Active & Passive Discovery.
- IP Probe
Nessus - Vulnerability Scanner
sqlthrash - doesn't exist
John The Ripper - Password cracking

WEP ——— lower security

WPA 2 ——— Better than WEP

- Enterprise mode
  Use RADIUS Authentication rather than preshared key

For consistent logging to SIEM

Use Group Policy, not windows client

Reactive Monitoring

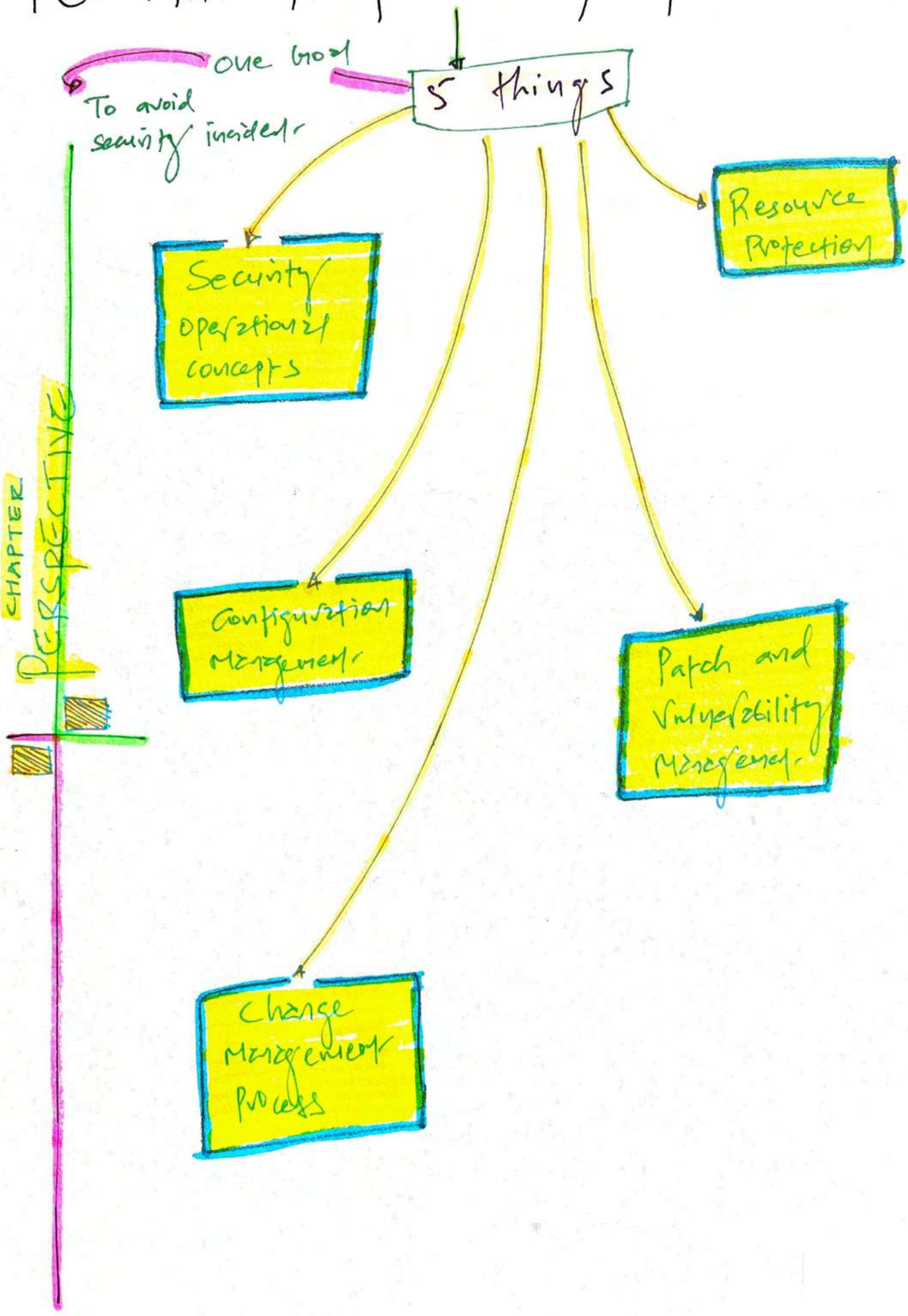
only works after issue has occured as it required actual / real-time traffic

Synthetic Monitoring

Use simulated / artificial traffic as proactive approach to identify issues before they occurs

only if it's in test script

16. MANAGING SECURITY OPERATIONS



APPLYING SECURITY OPERATIONS CONCEPTS

Senior Management → Responsible → Due Care
→ Due Diligence

Due Diligence: Taking good care of Information & Asset on ongoing basis.

Senior Management: Address Fundamental Security operation concepts to reduce the risk.

* Need-to-know (only permissions) & Least Privilege (Rights + Permissions)

Need-to-know (only permissions)

Focus on Permissions → Allows access to objects such as files

Allowed to go & read time

Associated with Security clearance

Dave has security clearance for secret data. It doesn't mean he can access all the secret data.

Admin provide access to limited secret data based on Need-to-know.

Least Privilege (Rights + Permissions)

Focus on privilege (Rights + Permission)

Rights refer to ability to take actions

Allowed to go & change the time

- This principle needs well defined job descriptions

When you control Privilege → it controls Confidentiality and Integrity of data

Admin doesn't mean Full control = consider only privilege

* Additional concept with Need-to-know and Least Privilege

Entitlement

Privileges we get when Account is set up for first time.

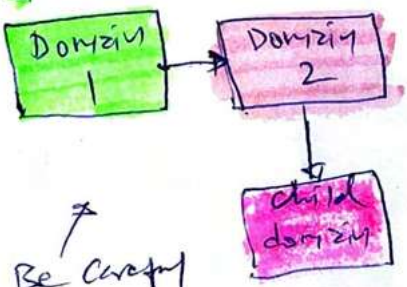
Aggregation

Privilege creep - user continue to gain privilege

↓

Revoke

Transitive Trust



Be careful

- Non-transitive trust enforce principle of least privilege.

* Separation of Duties & Responsibilities

Golden Eye +

Once Upon A Time In Mumbai

+ Movie Theatre ticket operation

Still chance of Collusion but takes more effort

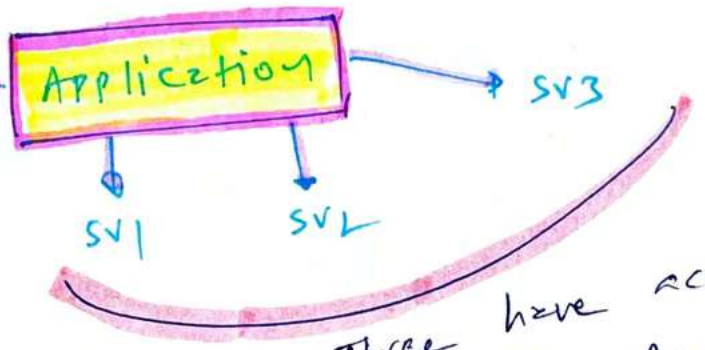
- Separation of duties ⇒ reduce fraud by requiring collusion

↓

Divide by security capabilities + functions among individuals.

Seperation of Privilege = Granular rights + permissions

Builds on top of least privilege Privilege → Apply to process + Apps



Three have access to specific functions within Apps = seperation of privilege.

Segregation of Duties

- Refer to (← P.T.O) movies + theatre example
- Goal = Restrict individuals having excessive system to reduce fraud.
- If seperation not possible = consider compensating controls to mitigate the risk

Require for SOX - Sarbanes Oxley Act

Two-person control = Holder Eye

Split knowledge = seperation of duties + two-person control

- Need 2 keys to open Box
- Need CEO + CFO to take critical business decision

* Job Rotation

As security control

As → Reduce Fraud

Cross Training

Act As → Deterrent mechanism — if employee know their someone will take their job role, they less likely to involve in fraud activity.

Act As → Detective mechanism

* Mandatory Vacations

To detect → Fraud

To detect → Collusion

Deterrent

Detection

* PAM - Privilege Account Management

Personnels don't have more privileges than they need & they don't misuse privilege

Elevated privileges can be misused to harm CIA of Assets.

Monitoring of privileged entities is important.

→ Tools available to Automate this

! - it can also detect Advanced Persistent threat (APT) activities

* Managing the Information Lifecycle

Protect Data → Based on classification

Security control → To protect information throughout lifecycle

Phases of Data in lifecycle

1. **Creation (capture)**
   - Either information is created or captured (from logs)

2. **classification**
   - Identify sensitive information based on classification
   - Marking (labeling) to recognize data value

3. **Storage**
   - Security controls based on data classification
     - (a) Prevent Unauthorised Access
     - (b) Encrypt Data
     - (c) Back-up
     - (d) physical control
     - (e) Environmental control

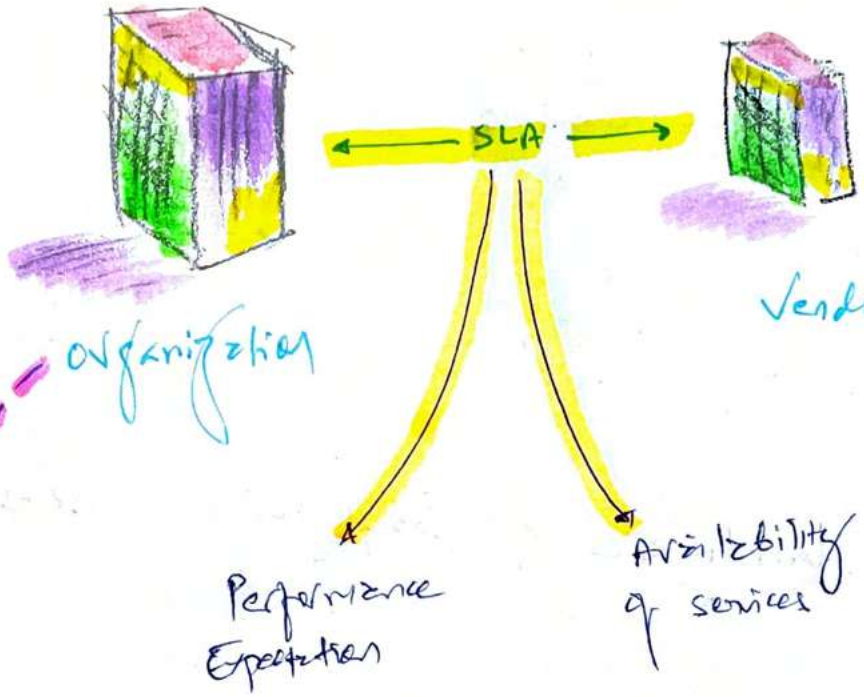
4. **Usage**
   - Data-in-use + transit = Encryption

5. **Archive**
   - Off-site data retention need same security control considerations

6. **Destruction (Purging)**
   - Sanitizing media
     - NIST 800-88 R1

* Service Level Agreements (SLA)

NIST 800-47



Also use **MOU** – Memorandum of Understanding + Interconnection

Not as effective as SLAs

ISA – Security Agreement

Used to define technical requirements (Encryption, Protocols) if two parties transmit sensitive data

* Addressing Personal Safety & Security

Duress

- Lonely guard can't fight with mob. He just press alarm button or play around with the phrase over phone "Everything is fine."

Emergency Management

- DRP (Ch: 18)

Security Training and Awareness

~~DRP (Ch: 18)~~

When Employees Travel = secure!

- Sensitive Data
- Malware & Monitoring Devices
- Free Wi-Fi
- VPNs

2

SECURELY PROVISIONING RESOURCES

Focus:
Provisioning + Management of

- H/W + S/W Assets
- Virtual Assets
- Cloud-based Assets.

* Managing Hardware & Software Assets

Hardware Inventories

- track hardware assets with barcode
- RFID expensive than barcode but reduce inventory time
- Sanitize H/W
- Treat portable media with table = include in inventory

Software Licensing

- Protect license key
- Ensure unauthorised software is not installed
  - SCCM can detect (configMgr)

Protecting Physical Assets

- Protect organization's building and contents
- Consider physical security controls.

* Managing Virtual Assets

Virtualization's primary software component → **Hypervisor**

Additional layer of software on physical server = introduce additional attack surface

Virtual Assets to

- VM
- VDI
- SDNs
- VSAN

secure

* Managing Cloud-Based Assets

NIST SP 800-145 + 800-144

- **SaaS**
  - Full service via web browser (Gmail)
- **PaaS**
  - H/w + s/w + Apps
- **IaaS**
  - cloud → Infra (server + storage) + networking resources
  - customer → Install + maintain OS + Apps

cloud Deployment

- Private
- Public
- Hybrid
- Community

* Media Management

↑ Is stored data secure?

FROM

- Unauthorised access
  - physical location
  - logical Access (technical controls)
- Environmental protection
  - Temp
  - Humidity
- Lable / marking to ensure CIA

* Tape Media

Don't expose to magnetic field = corrupt data (Erase)

2 copies
- on-site
- off-site (backup)

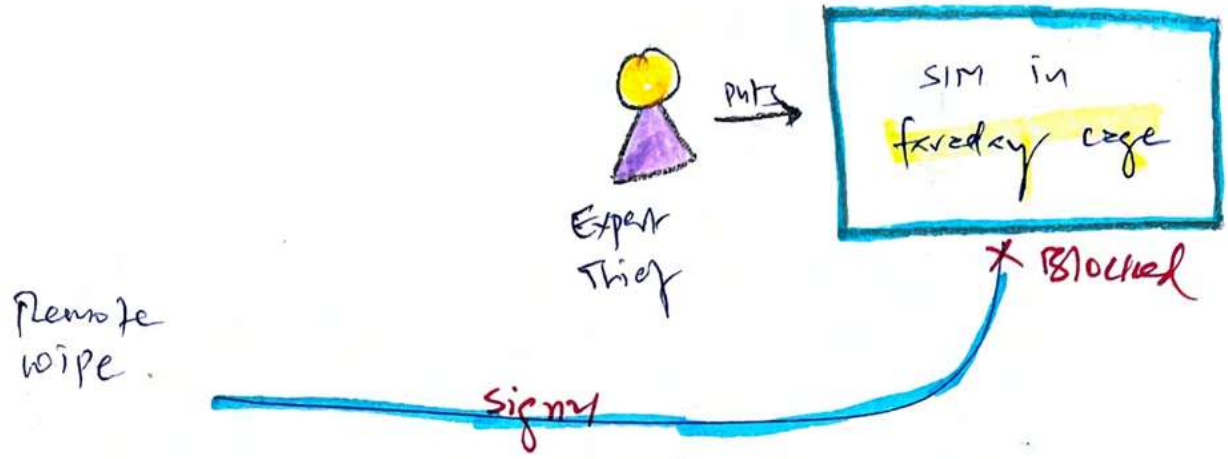
← Apply security Controls

* Mobile Devices

BYOD is challenging for organization → Moving to → CYOD

CYOD → Easy to manage + enforce security with MDM

→ Controls = Encryption, Remote wipe, MDS, Screen lock



* Managing Media lifecycle

When media reaches ⇒ MTTF (Mean Time To Failure)

MTTF value presents number of times media can be reused

Destroy Media

Destroy based on the classification

Sensitive = brutal destruction

SSD

Degaussing doesn't remove data — just burn the SSD!

MTTF vs MTBF (Mean Time Between Failures)

Can't repair after fail.

Time b/w failure to when personnel will repair it

3 MANAGING CONFIGURATION

Focus = Deployed systems are consistently secure throughout the lifetime

Baselining

- Achieve with secure baseline configuration for deploying images

Manual baseline = human error

Automate Tools ← Microsoft Group Policy.

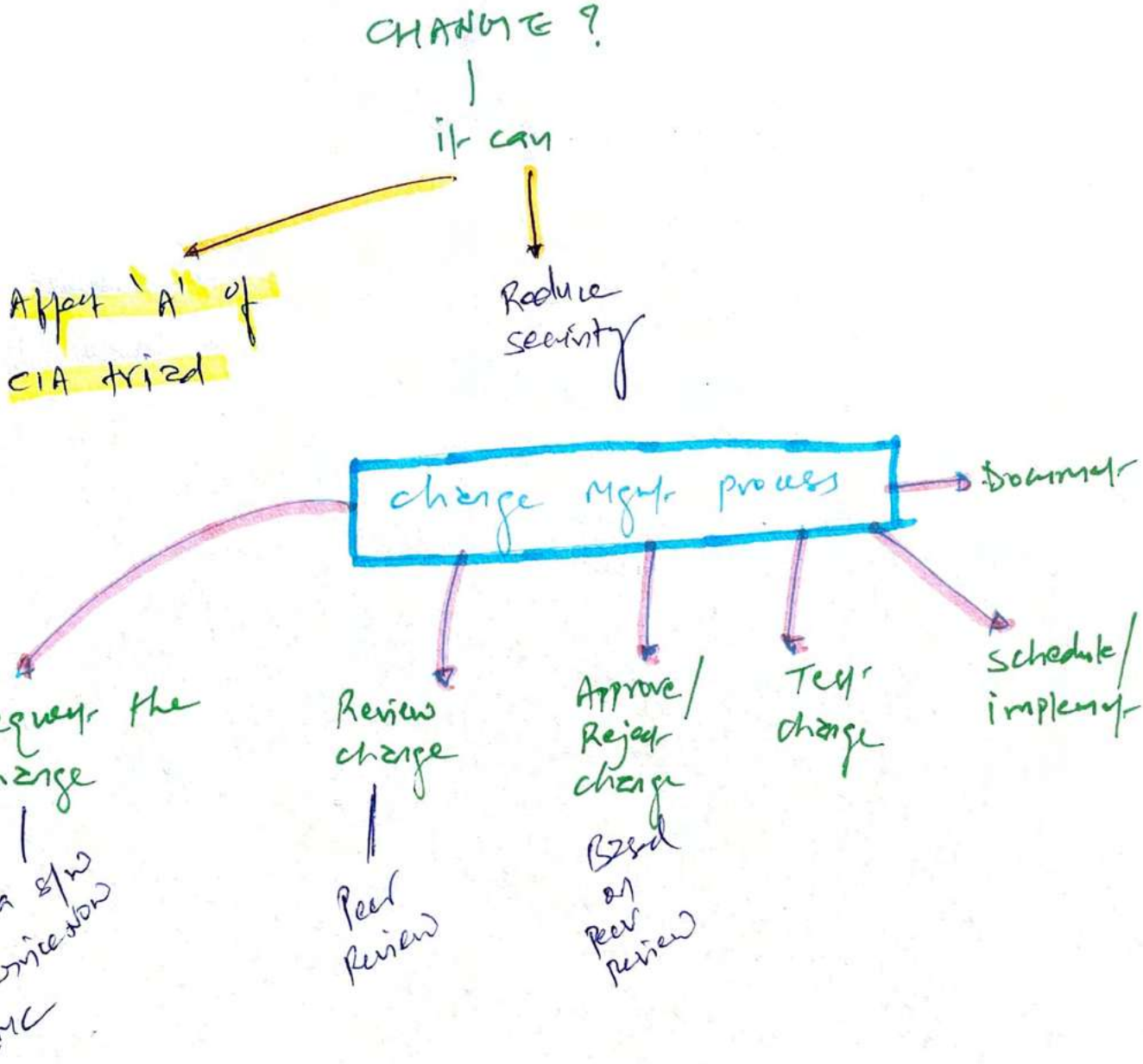
Using Images For Baseline (3 step process) ← protect from malware

1. Admin → PC
   - Configure OS with security
   - Test
2. Export to single Image from that PC.
3. Deploy secure image to all the systems

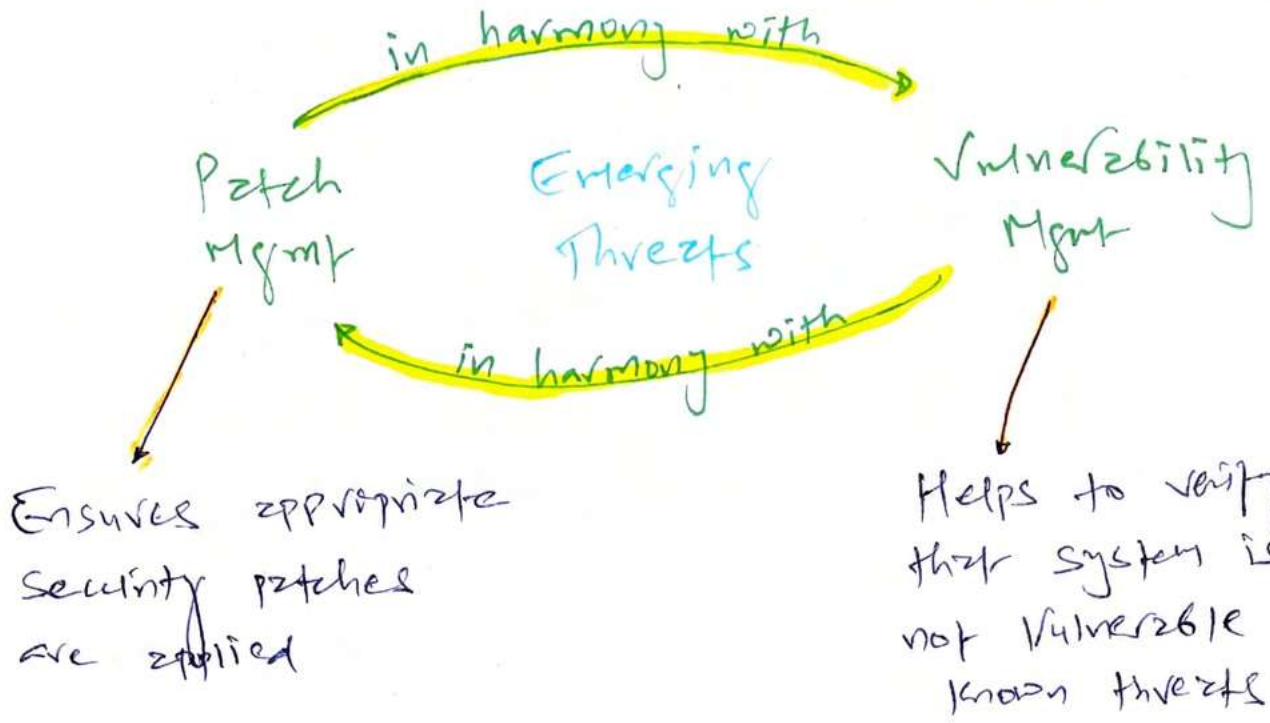
Benefits → security
→ less time = less cost
→ Easy to maintain

4 MANAGING CHANGE

Purpose: To reduce unanticipated outages caused by unauthorised changes.



5. MANAGING PATCHES AND REDUCING VULNERABILITIES



* Patch Management

Most of security incident → No patch mgmt policy.

Equifax attack in 2017

Effective Patch Mgmt program steps

- Evaluate Patches
  - Is it required for system?
- Test Patches
  - Test in isolated non prod
- Approve the patches
  - via change mgmt Process
- Deploy patches
  - Automated (wordpress plugin)
- Verify the Patches are deployed
  - Test & Audit with Vulnerability Assessment Tools (Tripwire)

* Vulnerability Management

Regularly identify vuls. → Evaluate them → Mitigate risk based on analysis

2 Elements

Vulnerability Scanning

Goal is to detect vulnerabilities & mitigate them before attacker discovers them.

- Uses database of known security issues - constantly updated for zero-day attacks
- Nessus / Rapid 7 = first scan open ports for services & checks for known system vulnerabilities

Nessus: Do more than scanning
- Database scanning for input validation

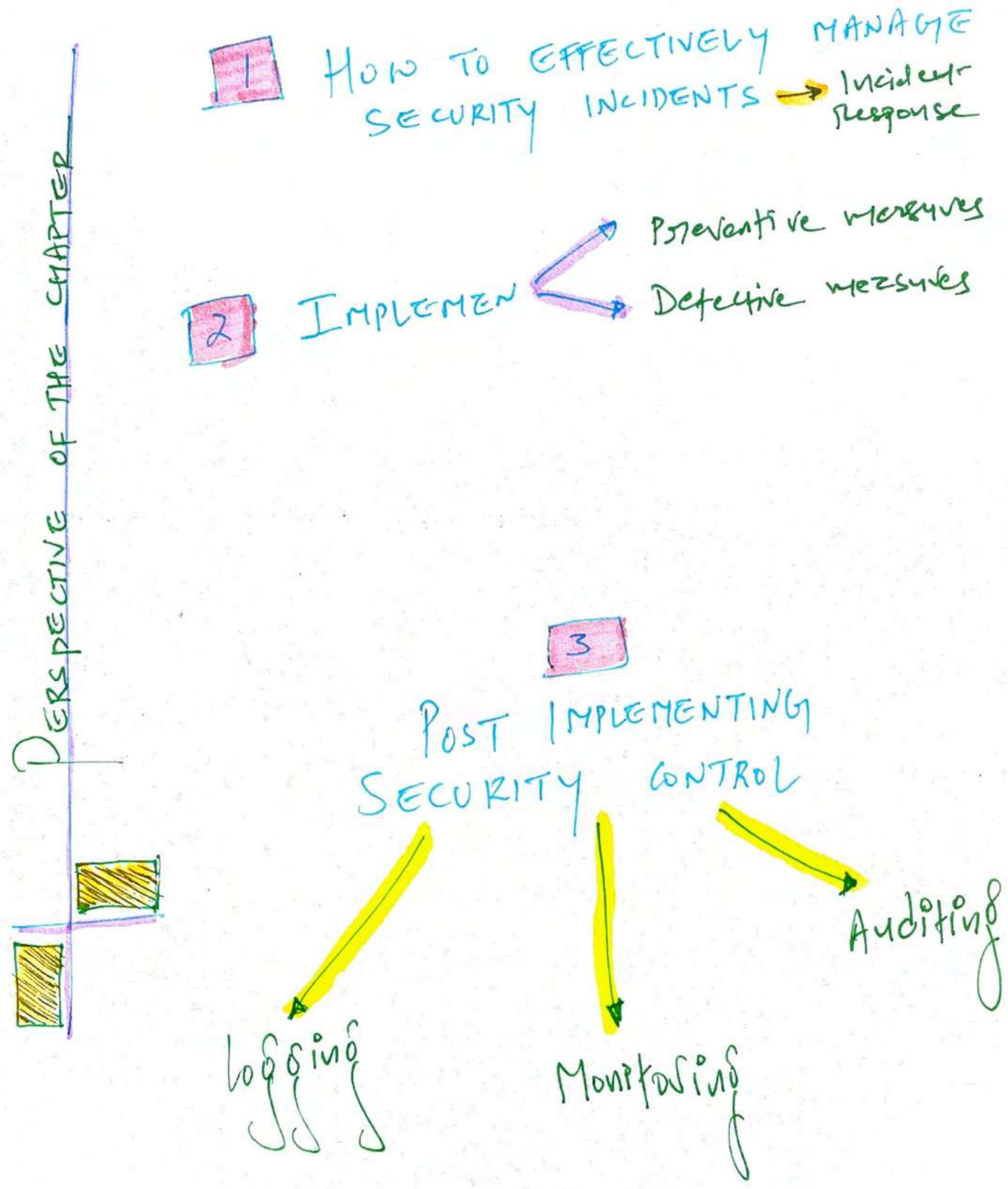
* Blame mgmt if they don't address vulnerabilities, or accept the risk.

Vulnerability Assessment

- Part of Risk analysis / risk assessment

1. identify value of assets
2. identify threats & vulnerabilities
3. perform risk analysis to determine overall risk

17. Preventing and Responding To Incidents



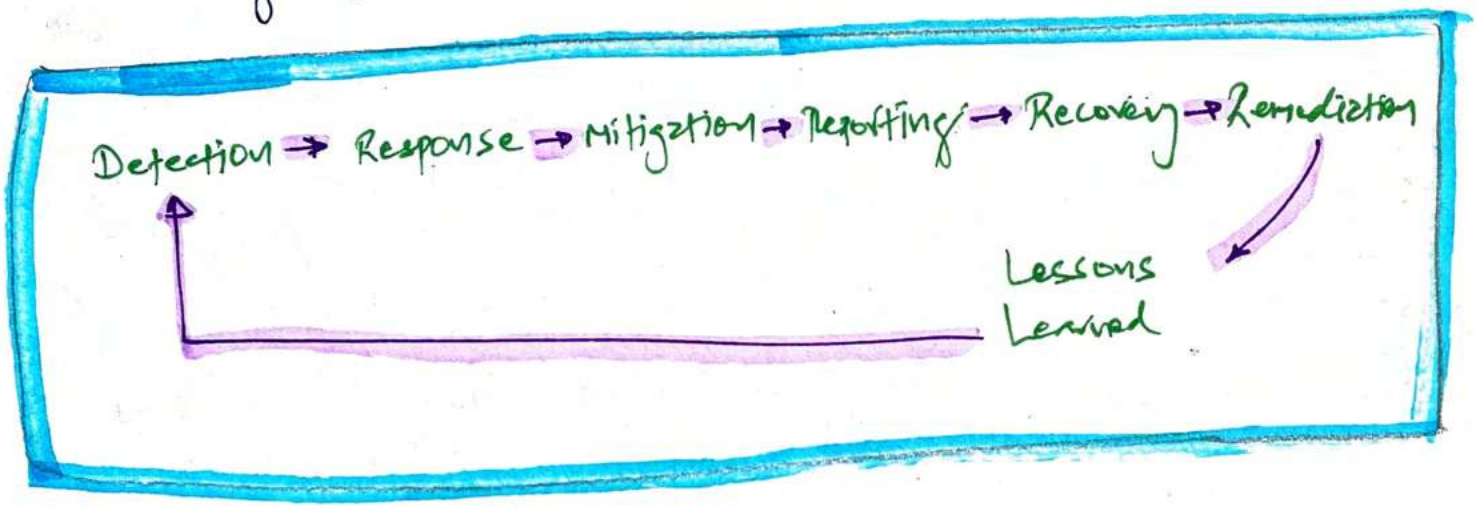
1 MANAGING INCIDENT RESPONSE

REVISIT
P.T.O
END

Incident mgmt
Primary Goal
- Minimize the impact of the organization

Incident Response Steps

Any event that effect CIA of organization's assets.



Few Important Points

↳ Incident response doesn't include counter attack as evil attacker may hide behind victim & our aggressive response may hurt the innocence.

(identification)

Detection - methods to detect potential incidents

From End User's observation on unusual activity

Human sensor

IPS | IDS

Technical sensor

Anti-malware

Automated scans / logs

SIEM

Train IT staff to differentiate which incident

Escalate

(Reduce) To prevent further damage

Goal

Troubleshoot

Investigate

From 3rd party

Threat intel sensors

Response = Quicker the better = containment

Tip
- Never turn-off PC when containing an incident.
- Temp file & data in volatile RAM will be lost that can be helpful to forensic team.

'A' of the CIA

Mitigation

Stop the contamination. Disconnect affected host from network & perform investigation.

Continue to mitigate without letting attacker know, monitor their activities + learn the scope of the attack

Reporting on breach → within organization, Especially upper mgmt

→ outside / media due to legal requirement or compliance

Reporting is crucial when it involves customer data. Remember Mark Zuckerberg investigation? :-)
(PII)

Many incidents are not reported because they don't recognize incident or key piece

↓

Solution = Training

Teach people how to recognize incidents.

Recovery — How?

→ minor incident = Reboot

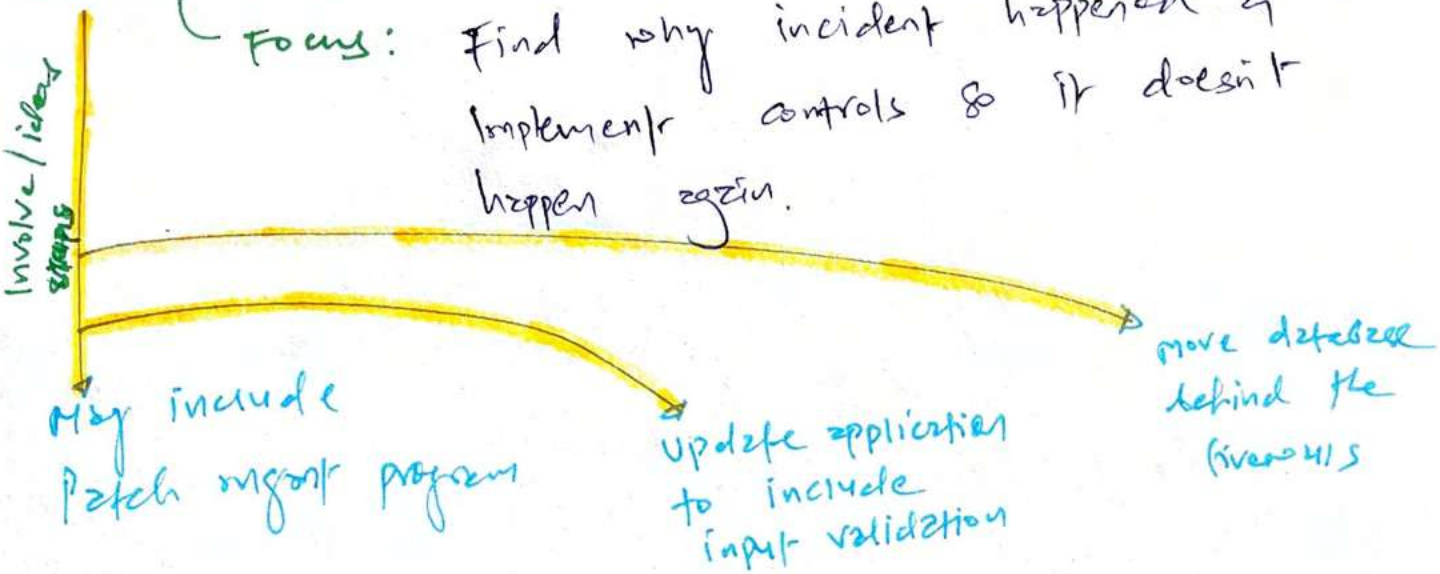
Major incident = Restore Backup + Rebuild the System

- Check ACL
- IAM
- Disable unnecessary services / protocols
- Install patches

↑ configuration mgmt + change mgmt policy will help

Remediations → Involves Root Cause Analysis

└ Focus: Find why incident happened & implement controls so it doesn't happen again.



Lessons learned : RETROSPECT

↳ Involves incident response team + employees that knows about incident

output feeds to detection

Also, feedback introduce new security controls or change to existing security policy & procedures.

2 IMPLEMENTING DETECTIVE AND PREVENTIVE MEASURES

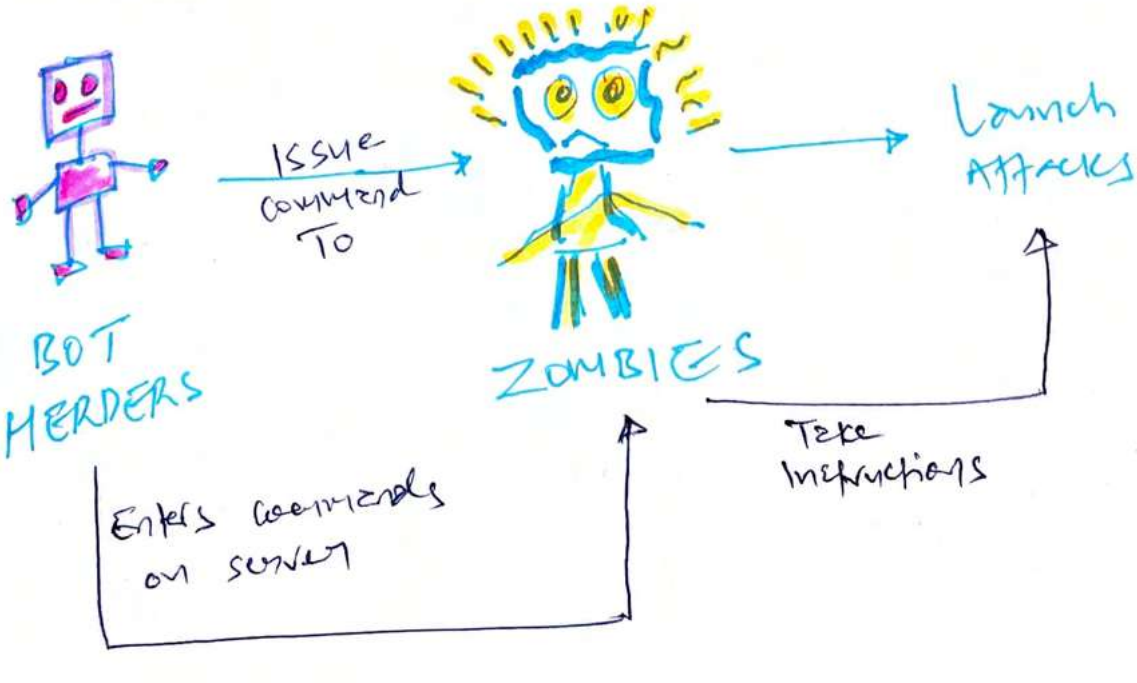
chapter Focus: Preventive security controls against well-known attacks

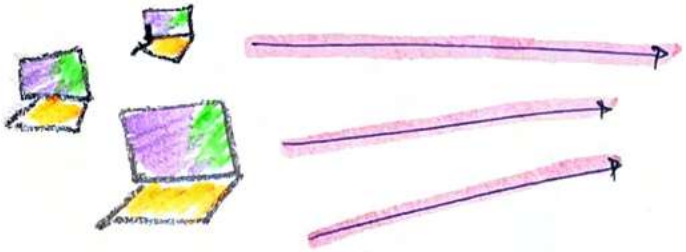
Basic Preventive measures → Disable unneeded service + protocol

- Firewalls
- Keep system + Application up to date
- IPS/IDS
- Anti-malware software
- Implement config. mgmt + system mgmt process

* Understanding Attacks

(1) BOTNETS — Robots





Affected PCs with malicious code

Joins

BOTNET

Botnet preventions

Defense-in-depth (multiple controls)

up-to-date Anti-malware software in System + Network

up-to date Browsers & plugins

Educate + Training users. DO NOT CLICK.

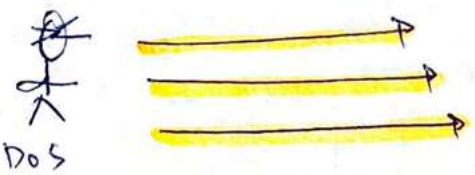
cyber sketch : Botnets for IoT

- Mirai malware (osg P 748)
- DDOS DNS Attack

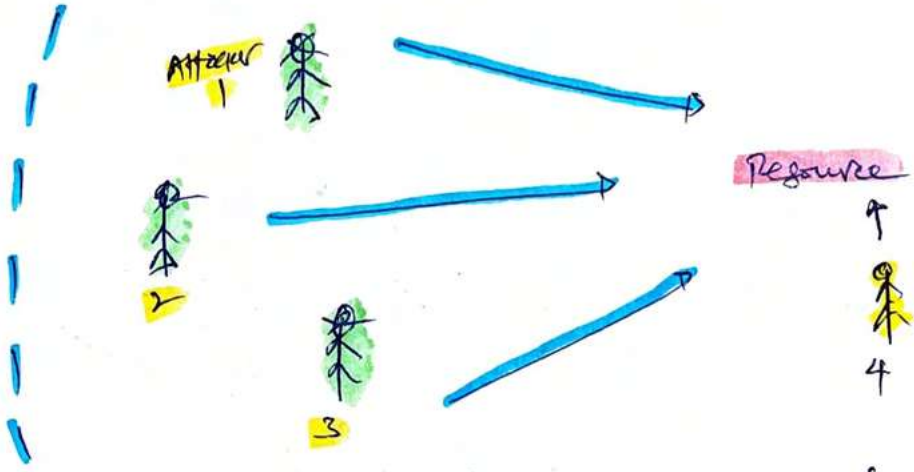
(2) DENIAL-OF-SERVICE ATTACKS (DOS)

Overwhelm resources

Exploit known vulnerabilities

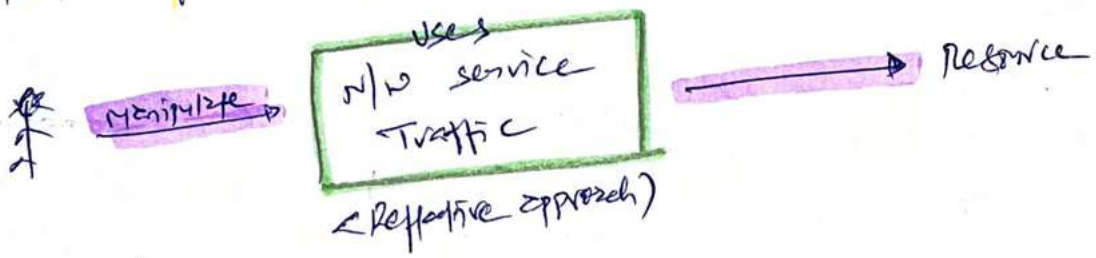


Distributed DoS (DDoS)



Attackers use BOTNETS to launch DDoS Attack.

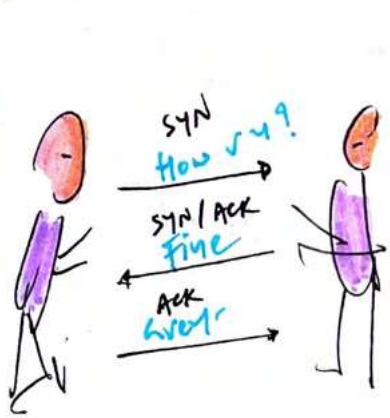
Distributed Reflective DoS (DRDoS)

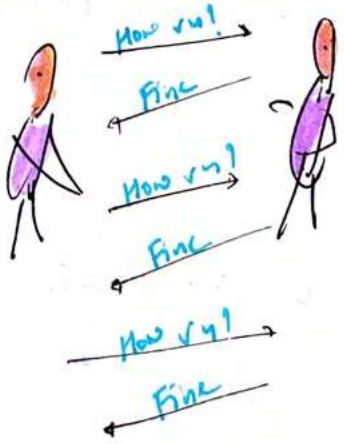


- DNS poisoning
- Smurf Attack

(3) SYN FLOOD ATTACK = DoS Attack

↳ it disrupts 3-way TCP Handshake





3-way Handshake

Syn Flood - Attacker never send ACK till resource is exhausted & no longer response to legitimate request.

Syn Ack Flood Prevention → Reduce the amount of time a server will wait for Ack. From 3min to 1min.

↓

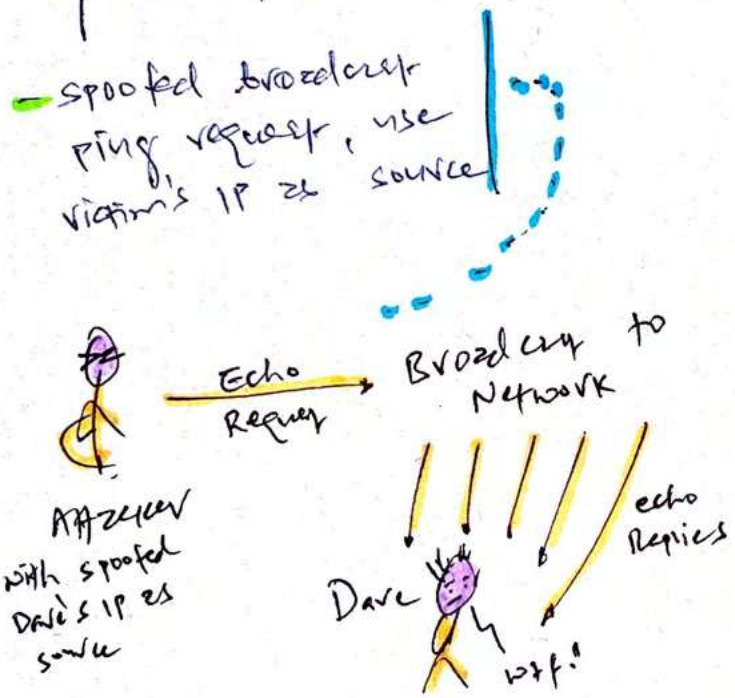
Session cookies

- Small reloads consume very few system resource

(4) SMURF & FRAGGLE ATTACKS = DoS Attacks

SMURF: Flood Attack = uses ICMP instead of TCP SYN packets

- spoofed broadcast ping request, use victim's IP as source



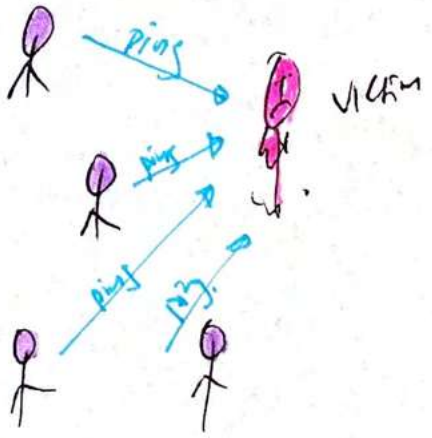
Prevention

- Block ICMP on routers + Firewalls
- correctly configure Routers / RFC 2644 compliance

FRAGGLE: Similar to smurf, but it uses UDP packets over UDP port 7 & 19.

(5) PING FLOOD

- Overwhelm victim with ping request
- Effective when zombie launches the attack within botnet as DDoS attack



(6) PING OF DEATH

Bigger PING packet

> 64 KB

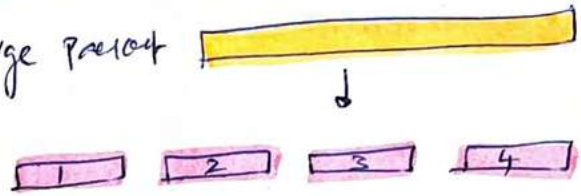
System crash

Buffer overflow

Sol:- patch

(7) TEARDROP

Large packet



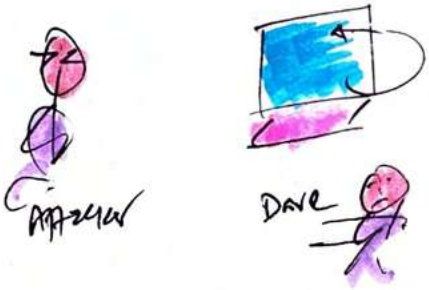
Attack

Coil. put the data back to normal

Sol:
+ IDS

(8) LAND ATTACKS

- spoof victim src + dest IP



- System reply to it self till crash, froze, reboot

- Sol. → up-to-date
→ filter traffic to detect identical src + dst

(9) Zero-Day Exploit

Attacker first discovers a vulnerability

Vendor learns of vulnerability

Vendor Release patch

- organization takes time to apply patch

Microsoft

Have patch mgmt policy

PATCH TUESDAY

EXPLOIT WEDNESDAY

Prevention from zero-day Exploits

- Disable unneed system service + protocols
- Enable IPS + IDS
- Deploy Host + N/w-based firewalls
- Honey Pots + Padded cells

(10) MALICIOUS CODE = malware = malcode

- Unauthorised activity
- Trojan Horse
- viruses, worms, Logic Bombs
- Destructive Macros

Methods

- Email Attachment — POPULAR !
- Drive-by-Download
  - Attacker modify website code.
  User visit, malicious code download.

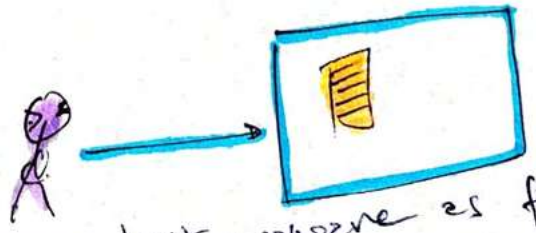
Takes advantage of unpatched systems.

uses

- Malvertising Ads

FREE TOOL MICROSOFT

- Install malware using Pay-per-install approach



Attack host malware as fake anti-malware to web hosting company.

(11) MITM — man-in-the-middle

2 types of attack

Sniffing (WiFi)

- copying traffic b/w two parties

Store-and-forward (Proxy mechanism)

- client & server think they are directly connected but attacker captures & forwards all data b/w two systems.

Prevention

- Use VPNs
- Up to date system with patches
- IDS - won't detect MITM, but can detect suspicious activity

IMPORTANT

(12) EMPLOYEE SABOTAGE

why did you fire me?

oh! I still have access after termination

AUTOMATE OFF-BOARDING

+ Intensive auditing + monitoring of unauthorised activity

RECOGNISE EMPLOYEES FOR THEIR CONTRIBUTION :)

(13) ESPIONAGE

└ LAPSUS$ tries benefit from this

- Dissatisfied employee turned to attacker or leak confidential data to criminal group

Prevention → Employee screening

→ Restrict sensitive data (security controls)

→ Traced back to Advanced Persistent Threat (APT)

Nex → IPS + IDS = IDPS

Inspects packet header + contents while Firewall only header (protocols).

As IPS also detects intrusion, they are called Intrusion detection & prevention system.

IDS

- records real-time monitoring of abnormal activity
- Actively monitor n/w traffic + inspect logs

IDS / Firewall / Antivirus software — provides Active response to security event / block traffic

while IPS — provides passive response & alert to admin, not a security event.

sensor on Router / Firewall → logs → IDS

Evaluates data & detect malicious behavior using 2 methods

Knowledge-Based Detection

- Signature based detection

can detect known attacks.

IDS vendor → Implements → Database of known attack

If logs → matches → IDS Alert

Similar to Antivirus signature
- Need constant updates
- if attack not in the database = no alert.

Behavior-based Detection

superior, can detect new attack but higher false alarms

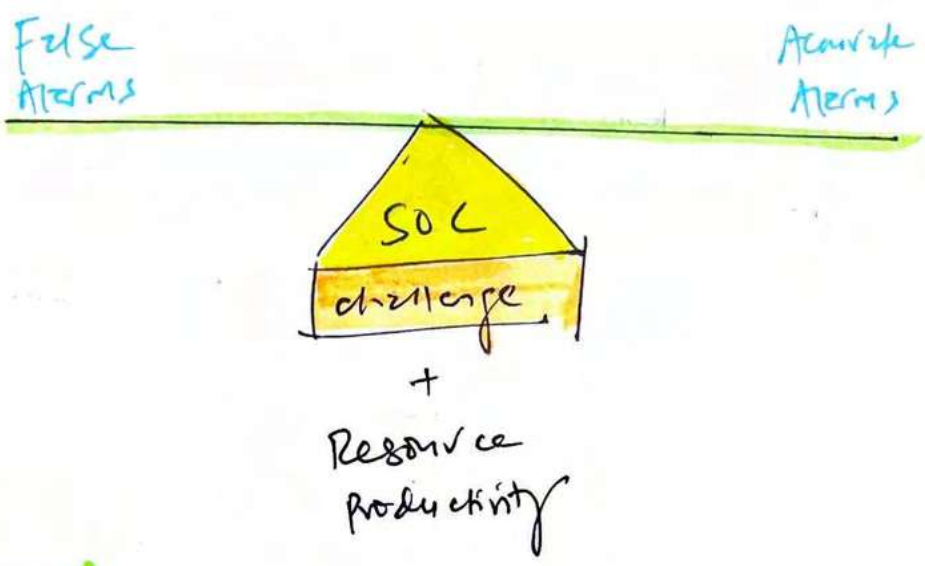
e.g.
- Statistical, anomaly, Heuristic-based detection

System → create BASELINE for normal activities + events

Realtime logs → (match)

if doesn't match = abnormal activity → IDS Alert

this is not the case here.



SIEM

Splunk / StreamDriven

Collect real-time data from multiple sources

Store data (long-term) for analysis

provide notification / Alerts of potential attacks

Keep it seperate from IPS / IDS

Converts Raw Data → Analytics Tools

IDS Response

① Event

②

Triggers alarm & respond with

Passive Response

- Ex: Email-Message (FYI)

Active Response

- Could be modifying Acl to block IP to respond SYN Flood Attack

IDs that use Active Response is IPS. sometimes.

IDS

HIDS
Host-Based IDS

- Monitors single host
- includes antimalware capabilities
- Detects anomalies on system that NIDS can't.

Application-Based IDS

- Specific type of NIDS for specific application

NIDS
Network-Based IDS

- Install sensor on core networking device & send logs to SIEM or central console
- Can monitor large network

Disadvantages

- Costly + hard to manage
- intruder can disable HIDS in system
- can't detect network attack
- consume significant system resource

Disadvantage

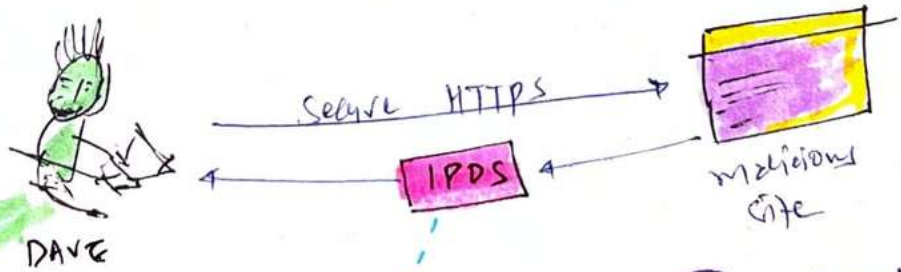
Can't go HIDS → want granular

- Can detect buffer overflow exploit in Network but which system, file, resource, application?

OSG P. 760-761

75% traffic on Internet is encrypted. Good to protect data but challenging for IDS. How?

cyber attack



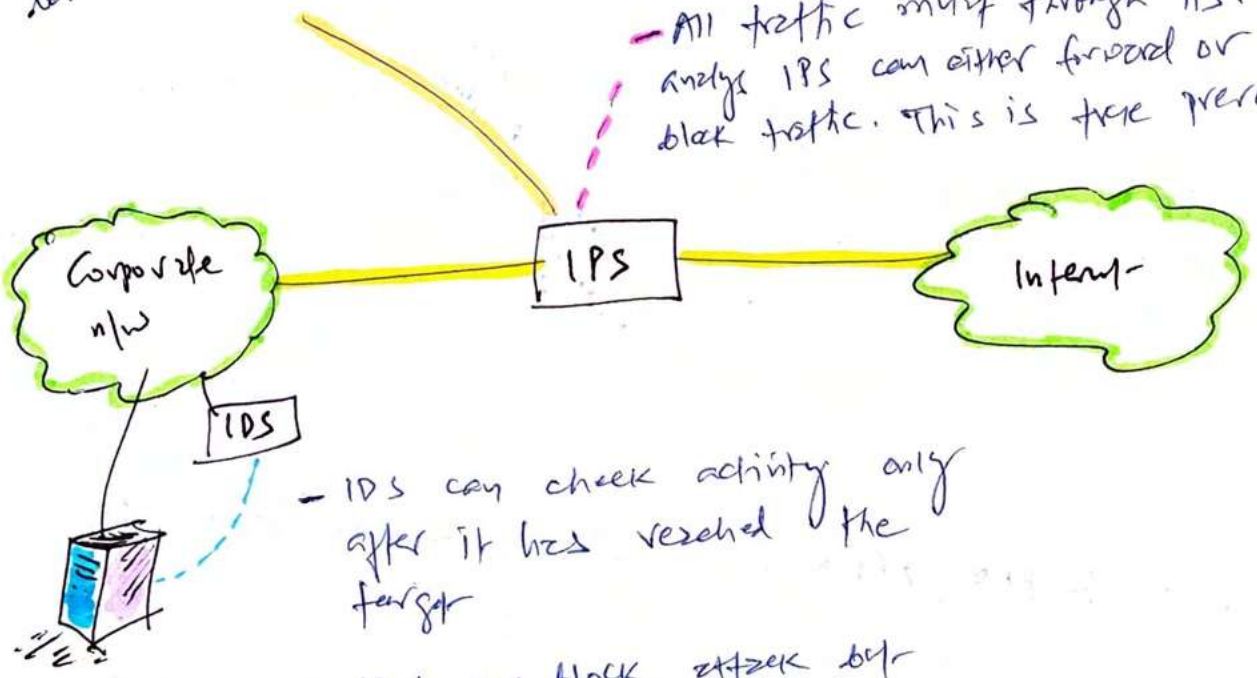
SOLUTION — can't detect malicious code] ...decrypt → IDPS

USE OF TLS DECRYPTORS ← This is what DLP does!

IPS = IDPS

→ special type of IDS that detect & block attacks before it reaches to the target system

Can use knowledge-based | behavior-based detection.



- IDS can check activity only after it has reached the target
- IDS can block attack but it can't prevent it

* SPECIFIC PREVENTIVE MEASURES

↳ implement on top of IPDS

Honeypots / Honeynets ---

Individual PC as trap for intruder

Network of Honeypots

Goal: Distract intruder from legitimate systems

Honeypots are good because

- Allows to monitor Hackers activity
- creates delay so IDS can gather more information
- For detecting zero-day Attacks - used as countermeasure

Use of Honeypot = Enticement & Entrapment issues

Enticement: Put vulnerable system in public & let hacker exploit

Prostitutes (illegal but intentional)

Entrapment: Encourage someone to do illegal & charge them

prostitute charges Force Rape over

Pseudo Flaws (FALSE VICTORY)

- Convince the attacker that they have gained access / successfully hacked the system.

But, it alert the ADMINS

Padded Cell

- Similar to Honeypot but performs Intrusion isolation approach.
- Simulated quarantine environment where fake data is provided to learn more about intruder & type of attack.

Warning Banners

- Signs for authorised & unauthorised users
- Deterrent control

Anti-malware

- up to date signature files + heuristic capabilities

Update / week → / 2hrs

Then

s/w focus on viruses

Now

Trojan Horse
Spyware
Rootkits
worms

Have Multipronged Approach to Block Malware

- Anti-malware on Email servers
- Firewall with content filtering capabilities at Perimeter
- On individual system (E.g. to block USB drive)

Also

- Incorporate principle of least privilege (Restrict user to install applications)
- Educate users about the dangers of malicious code

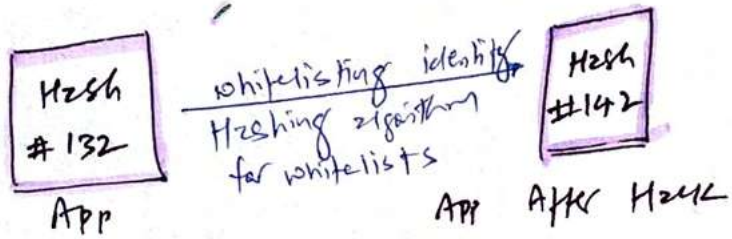
Whitelisting & Blacklisting = Goal: to prevent users running unauthorised Apps / prevent malware infections

Authorised Apps

Unauthorised Apps

Apple is extreme use case.

We can only install iOS on iphones/ipad.



Firewalls

- Basic
- 1st Gen
- 2nd Gen
  - filtering capabilities
- 3rd Gen
  - stateful inspection
- Nextgen.
  - Function as UTM (Unified threat management)

Sandboxing

Uses virtualization technique

To test application - isolate from host & network

2 techniques

1. When dealing with unknown apps
2. Anti-malware software

- Most anti-malware vendors uses virtualization as sandboxing technique.

Third-party Security Services

Security outsource ? we can opt follow compliance — PCIDSS

Preventive Measure

Penetration Testing

- DoS Attack
- Database for SQL injection
- Vul. scan
- Social Engg Attack
- port scan

PenTest Risks

- Keep AVAILABILITY in mind as it can cause outages
  - Do via change mgmt / After hours
- Perform in Non-prod / Sandboxing
  - challenge: won't get true value of prod environment
- Always get a written confirmation from upper mgmt for Pen testing

PenTest Techniques

Black-box testing
By Zero-knowledge Team

$$$$

- simulates real external attack

Black → No knowledge
White → Full knowledge

White-box
Full-knowledge Team

$$

- crystal-box / clear-box testing
- cost effective + efficient for locating vulnerabilities (~~less~~ save time in discovery)

Gray-box

- Partial knowledge Team

Protect Reports

Pentest Reports = classify as Sensitive + implement security controls

Mgmt to decide from report FOR NEXT ACTION

- Implement controls!
- Accept the risk.

Ethical Hacking

Hacking with legal terms.

Crackers, Attackers

↑

Malicious / Bad ones

↑

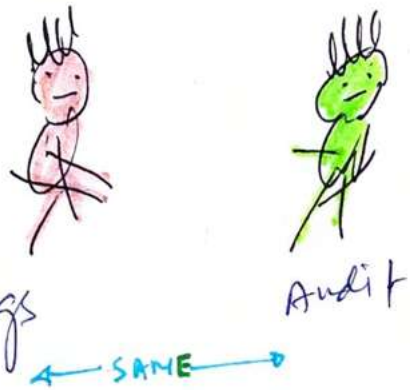
Hacker (Good one)

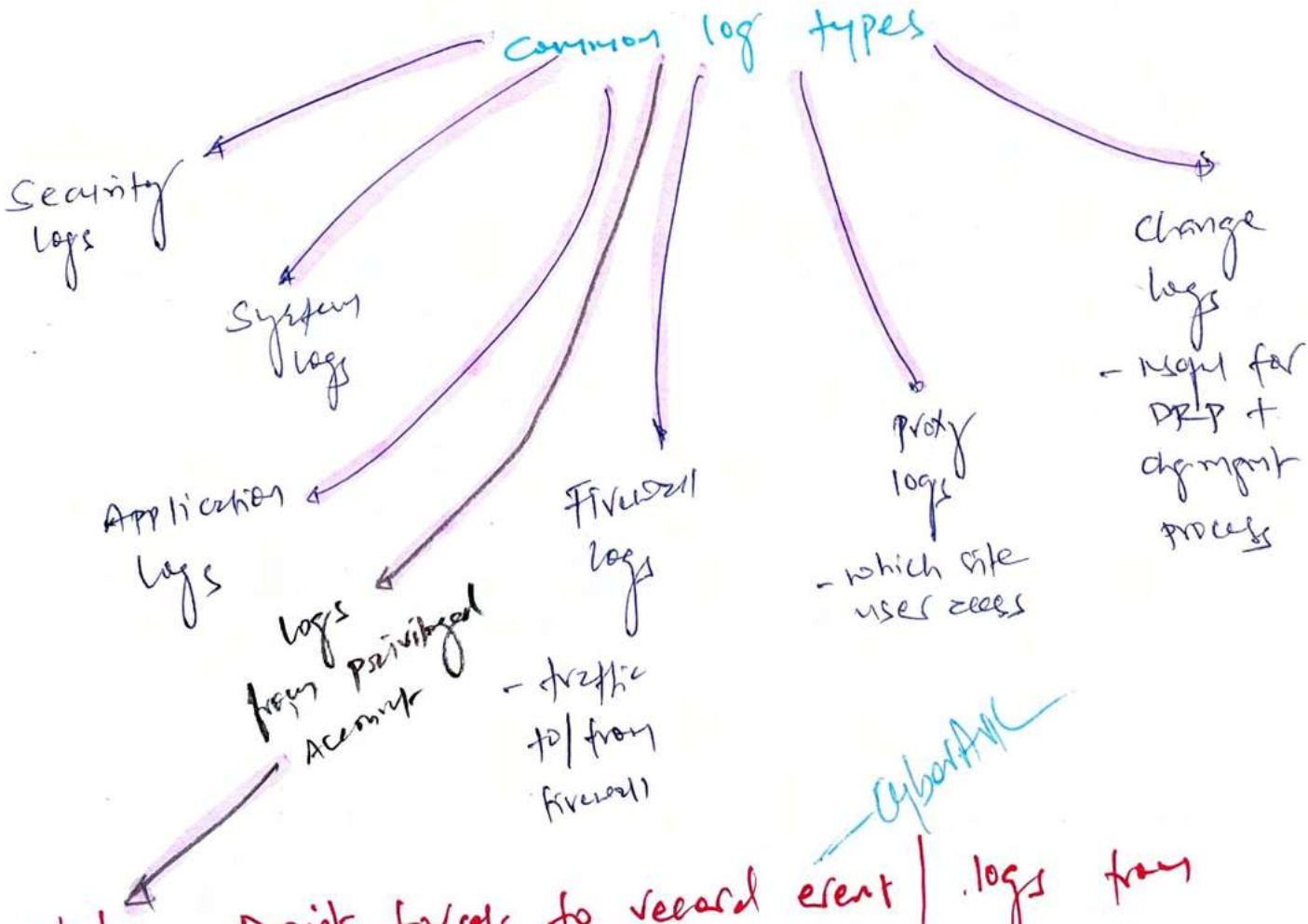
3 LOGGING, MONITORING, & AUDITING

Focus: Need LMA to prevent incidents & provide effective response when they occur.

+

Helps to reconstruct activity after the event has occured to identify what happened





Note - Don't forget to record event / logs from CyberARK

Privilege / root accounts. This prevents attack from malicious insider

Protect log Data — How?

Store backup copies of logs on central SIEM in case attacker delete/modify logs

Security policy for backup logs + retention + destroy logs after retention

SO, SIEM can backup logging data — cool!

Restrict Permission/access to

log files

The Role of Monitoring

P.t. 0

AUDIT TRAILS

- Passive form of detective security control
- ~~like~~ Deterrent like CCTV
- Info. about events stored in more than one database files

Postmortem

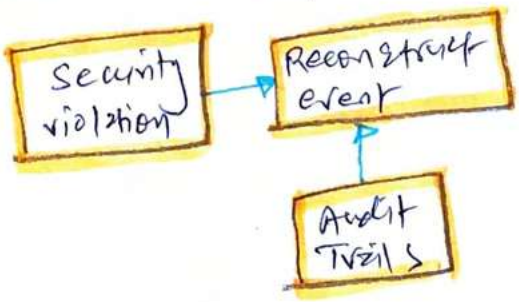
- Reconstruct activity - forward or reverse order to find culprit - or why exactly happened.
- As evidence for prosecuting criminals

MONITORING & ACCOUNTABILITY

- People can fool around "authentication" but "accounting" never lies.
- Always monitor users so we can hold their actions accountable.

no monitor = no accounting = no proof if they F**up.

MONITORING & INVESTIGATION



Most imp = NTP config.

Ensure logs have accurate time stamps. = NTP

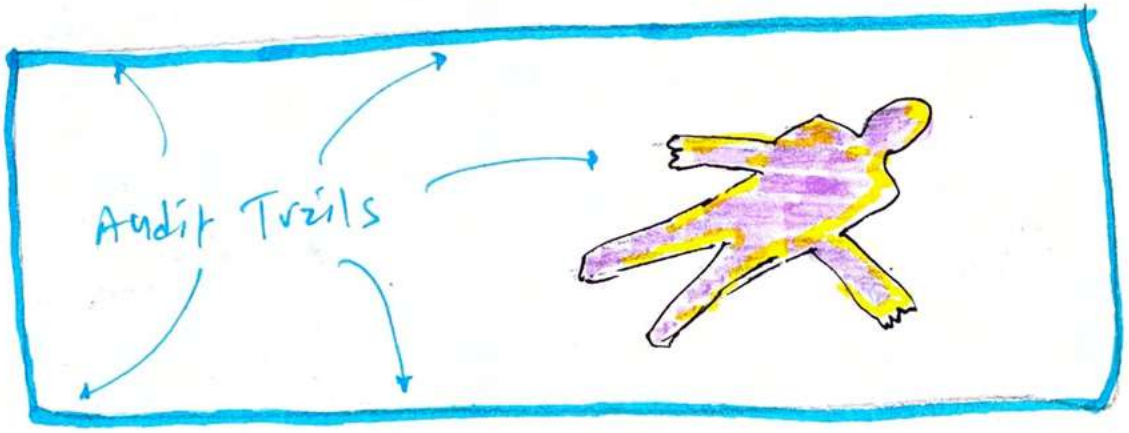
After NTP, NIST servers responds with encrypted & authenticated time messages.

MONITORING & PROBLEM IDENTIFICATION

When victim dies, it leaves more than one clue for investigation

Audit Trail / Log file has details to identify problem.

- OS failure
- s/w error
- system failure.
- traces of malicious code



MONITORING TECHNIQUES

monitoring

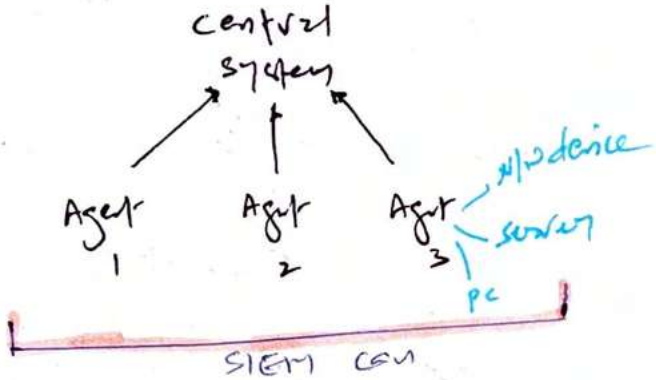
- manual review logs
  - overwhelming?
- Automate process
  - s/w automatically look for abnormal / suspicious activity.

$$$$ SAMPLING (Data Extraction)

data Reduction

- Extract specific data from large to present something sensible
  - there is always risk for accuracy.
- Use statistical sampling for precise & accuracy

(Security Information & Event Management) SIEM



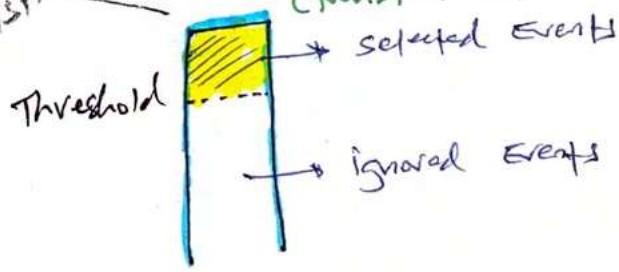
E.g Monitor group of Email servers

can collect logs from target system and use data-mining technique to retrieve relevant data.

Advanced Analytics to detect abnormalities + send alert to Admins

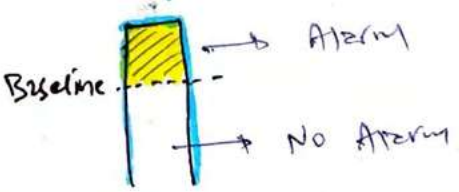
Inventory & software monitoring to detect unauthorised s/w or unapproved s/w

NON Statistical $$ CLIPPING LEVELS (Nonstatistical)



E.g - Failed logon Attempts

* clipping levels = used in process of auditing events to establish baseline of system or user activity.



- Select events that exceeds clipping levels.

OTHER MONITORING TOOLS

CCTV

Keystroke Monitoring

Record keyboard activity

video

H/W

S/W
- Keylogger

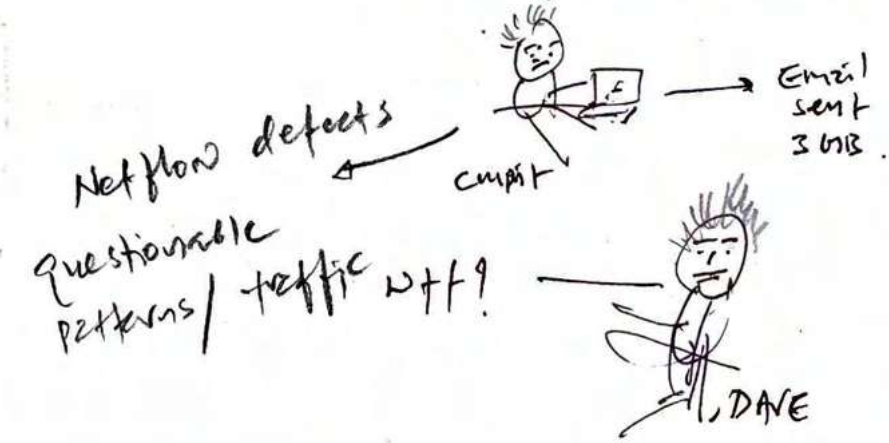
Required to inform employee before monitoring.

Traffic Analysis & Trend Analysis

- Forms of monitoring focused into flow of packets, not the content of the packet.

NETFLOW

- Network flow monitoring



Egress Monitoring

Data leakage

How to prevent Data Exfiltration?

Unauthorised traffic going out

DLP

Steganography

Watermarking

DLP - DATA LOSS PREVENTION

Network - Based DLP

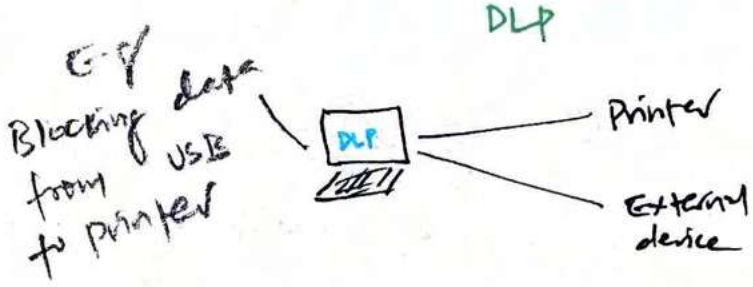
- Scan all traffic going out looking for

* Keyword * classification * filesize
* Filetype (MP3) * pattern * watermarking

Generate Alert → Admin

Need TLS decryption

Endpoint - Based DLP



- Scans files on system + traffic going out of system

Note :- DLP doesn't have ability to decrypt data. It scans only unencrypted data.

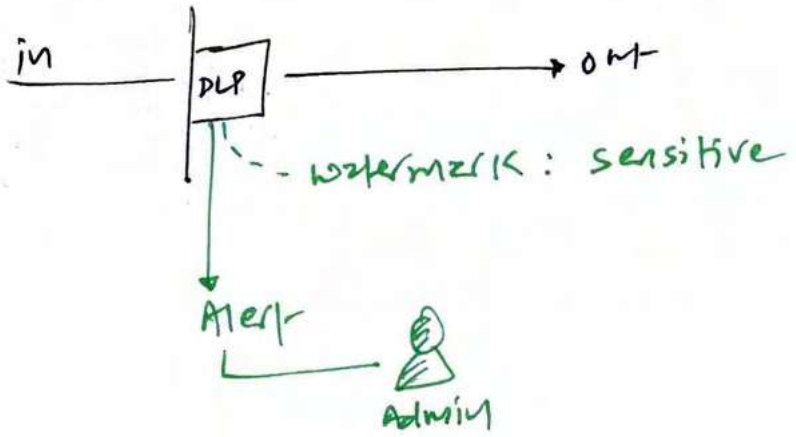
STEGANOGRAPHY

- Practise of embedding message within a file.

* Using SHA-3, we can compare hash of original & file with hidden message. should come with same hash value.

WATERMARKING + Egress monitoring

→ From DLP perspective
- they can detect "watermark" in unencrypted file.



Studio, Movies use digital watermarking when sending copies to distributors

* Auditing to Assess Effectiveness

↓

Not everybody knows about SECURITY policy

we have to

AUDITING → 2 meanings <P.T.O>

AUDITORS

They
- Test & verify Auditing process

Is policy providing security like it's meant to be?

Are people following security policy?

Are there any holes in security solns?

Auditing and Auditing

Use of Audit logs & monitoring tools to track activity.

Inspection (Evaluation) of process / security policies / Guidelines / procedures

* **Inspection Audits**

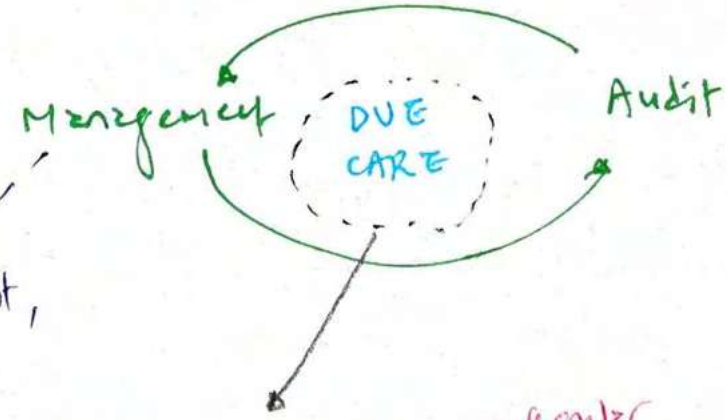
Two important Audits in the context of Access control

Access Review Audits → P.T.O

User Entitlement Audits. → P.T.O

Audit = time * money

Frequency of Audit ∝ Risk



that fails Audit, fails due care.

Note - For mgmt, regular security Audits are Due care, if they fail, hold them accountable for any Asset loss. (data)

Access Review Audits

- Purpose: verify that users don't have excessive privileges and accounts are managed appropriately.
  - Ensures process + policies are in place, working & people are following.

→ Access review verifies that policy exists and personnels are following it.

E.g restricted data
- is it classified?
- who has access?
- where & how is data stored?

User Entitlement Audit

leverages the principle of least privilege

- Reviews which users have excessive privileges
- which security policies are violated related to user entitlement.

while,
User entitlement audit detects whether processes are in place to remove privilege when user no longer need them.

AUDITS OF PRIVILEGED GROUPS

- Not everybody should be part of Admin AD group.
- Admin group members use high-privilege accounts when necessary.

Note - Automate membership for privilege accounts in group. So, no one can add or modify manually. ↑ unauthorized user

Dual Admin Accounts

90%.
Admin 1

- Day to day Activities

10%.
Super Admin

- Additional privileges

if Auditing finds = SuperAdmin is used 100%.

⇓

Security policy violation

* Security Audit & Reviews

Purpose : To ensure that organization has implemented Security controls properly.

From context of Security operation Domain : Security Audit help ensure that management controls (Administrative controls) are in place.

some items to check

- **Patch Mgmt**
  - Vul. scan report helps here
- **Vul. Mgmt**
  - Helps to identify & mitigate vuls.
- **CFG. Mgmt**
  - Ensures original configuration is not modified
- **change Mgmt**
  - Ensures change is implemented as per chg mgmt policy

they are all policies --

* Reporting Audit Results -

Why to include in the Report

- scope of audit
- Purpose of Audit
- Discovered results / Revelation from Audit

- - - - How to protect Audit report?

- classification
- Least privilege / RBAC

How to distribute?

- Follow / Refer security policy

* External Auditor

- Issues Interim report: When problem or issue is too important to wait until the final Audit report.
- Holds EXIT CONFERENCE at the end to demonstrate findings, investigations & recommendations.

<Don't refer this - P.T.O RITUALS>

INCIDENT MANAGEMENT — Proactive & Reactive process

P.T.O end

Security incident - Declare when IT operation disrupt or we have evidence for breaking security policy

To prevent incidents & detect quickly

Detected incidents dealt properly

1 DETECTION

Identification

Implement three types of sensors for detection

Noticing odd Events — Human

SIEM, IPS/IDS — Technical

Alerts from supply chain partners — 3rd party

Analyst receives alert from detection system & verifies the accuracy.

P.T.O

2. RESPONSE

Containment → Goal:

To prevent or reduce further damage from incident so we can begin mitigate & Recover.

How?

RESPONSE strategies

Indicate to Attacker that attack has been noticed & countermeasures are in process ---

Target isolation first if possible | containment

If not → Don't power-off system for forensic evidence

change FW rule or apply ACL to minimize the exposure

Deploy Honeypot as we need more data from attacker to perform root cause analysis later

3. MITIGATION

Eradication

→ GOAL : We reduced the exposure in step 2 but it's time to properly mitigate the threat by understanding the cause.

Who is the Attacker!

What is he after!

Exactly, how many systems are affected?

End of this step : Determine cause & system so we can process toward rebuilding system to good state

4. REPORTING — refer to original notes

→ Initial report → Governing Bodies

- Upper mgmt / Stakeholders
- Internal users
- External clients / Partners

7. LESSONS LEARNED

5. RECOVERY

- Refer to original notes
- Get business-as-usual with change mgmt + Backup / restore

6. REMEDIATION

- Perform root cause Analysis & develop security controls to prevent future attack
- GOAL : Now we have security implemented for such types of attacks.

How do you know – when to call a SECURITY INCIDENT

- IT operation / Business operation disrupts
- Breach of organization's Security policy
- Any intrusion attempt on network or anywhere that targeted company
- Malware infection

from Pituic
Revised incident mgt process – P.T.O

detection / triage

1 – ~~identification~~ / Triage

2 – mitigation & containment & Eradication – isolated from n/w

3 – response – Alerting team & responding to incident (SOC Analyst)

4 – Reporting – telling senior

5 – Recovery – chg mgt

6 – Remediation – root cause analysis

7 – lesson learnt – bring diff. department – to improve process

FROM RITVIK: Incident Management (Response) process.

1. Detection / Triage
   E.g Unauthorised access to system is identified.

Response

2. Mitigation / ~~Containment~~ / Eradication
   E.g All Access to system is revoked & system is disconnected from the network

3. Response (containment) — Mitigation
   SOC
   Gathering team to respond to every

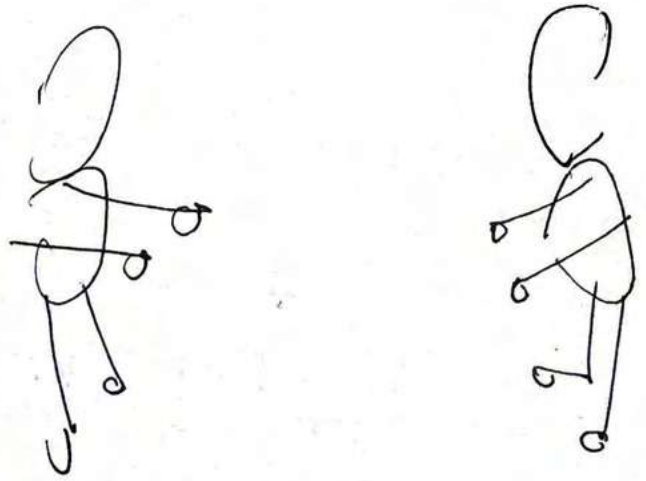
4. Reporting
   - ~~Restoration of effected system~~
   - update senior mgmt.

5. Recovery (Aim is to get back to Business)
   - Restoration of effected system
   - change mgmt policy - Business as usual Recovery.

6. Remediation (Then Go to the bottom of the issue)
   - Root cause analysis.
   - implementing controls to prevent future incident

7. Lessons learned.
   - Retrospection: Bring different department to improve process.

18. DISASTER RECOVERY PLANNING



Ch: 3

BCP ------ DR ---- This chapter

2 Brothers

↓

Same work

↓

Back to Business

PERSPECTIVE

DR = Technical controls

Prevent disruptions + restore service as quickly as possible

THE NATURE OF DISASTER

When

I.T = helpless to support mission-critical processes

↓

DRP kicks in

To manage the restoration and recovery procedures.

Plan = Autopilot

↳ less decision making in the event of the disaster

Anything that disrupts normal IT function

Disaster forms

Natural Disasters

- Earthquakes
- Floods
- storms
- fires

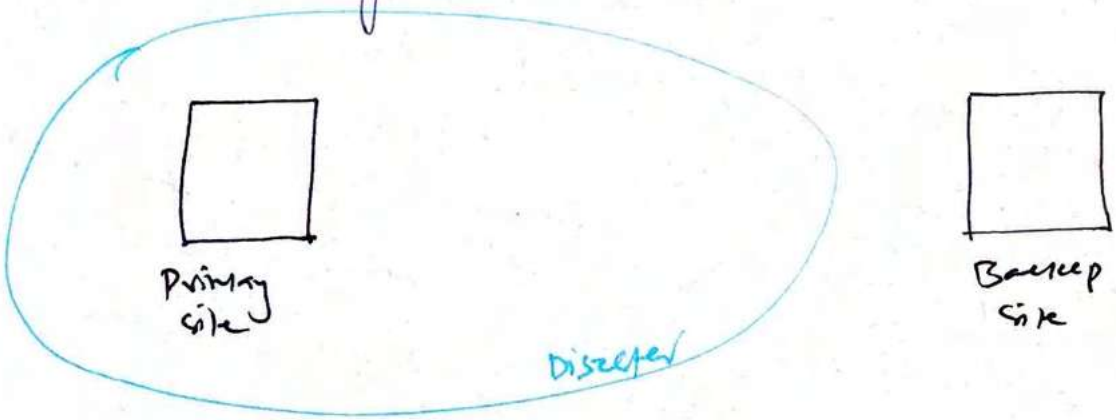
Man-made Disasters

+ Hacking

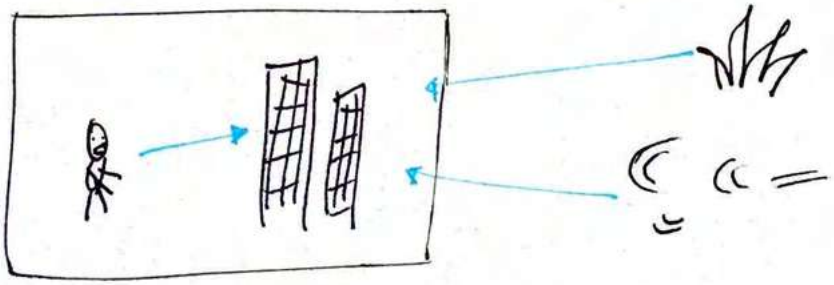
- Fires
- Terrorism
- Bombing / Explosions
- Power Outages
- N/w, Utility & Infrastructure failures
- H/w + s/w failures
- Strikes / picketing
- Theft / vandalism

Remember → visuals

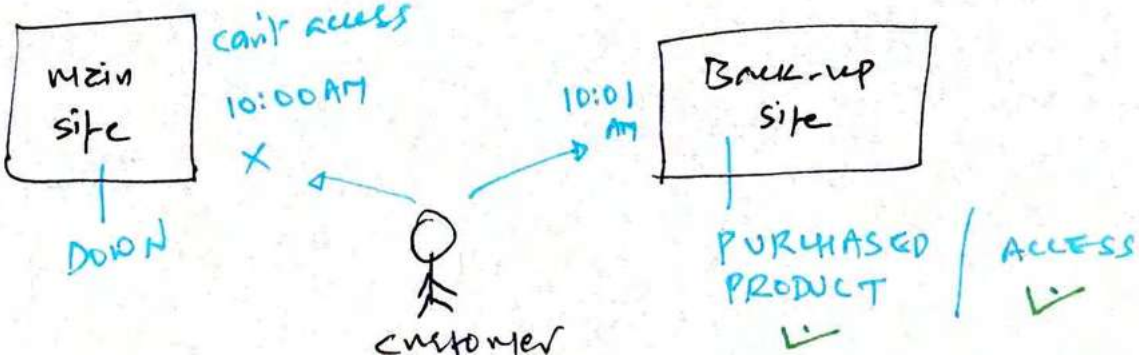
(1) Alternate processing sites are far enough away from main site that they are unlikely to be effected by same disaster.



(2) Threats to organisations are internal & external



(3) Disaster strikes without warning. Be prepare to operate backup site as primary in moment's notice.



UNDERSTAND SYSTEM RESILIENCE AND FAULT TOLERANCE

Goal

To eliminate single-point-of-failure (SPOF)

Fault tolerance -
Ability of system to suffer a fault but continue to operate.
(Not only being available but also allow access to data)

Can run 2K during covid-19 injection

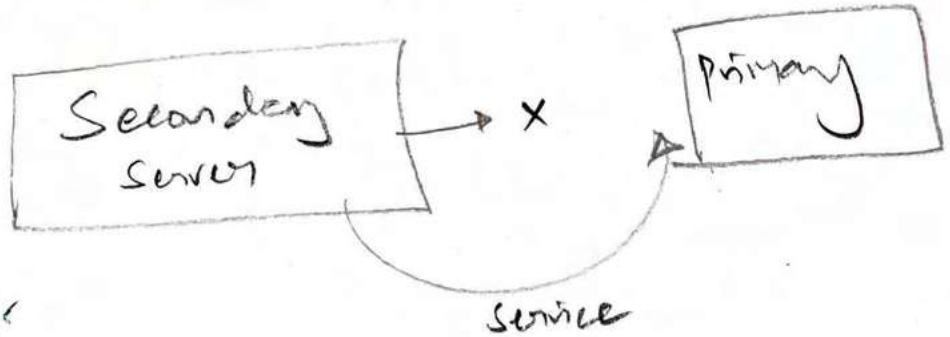
System
Ability to maintain acceptable level of service during an adverse event.

(or)

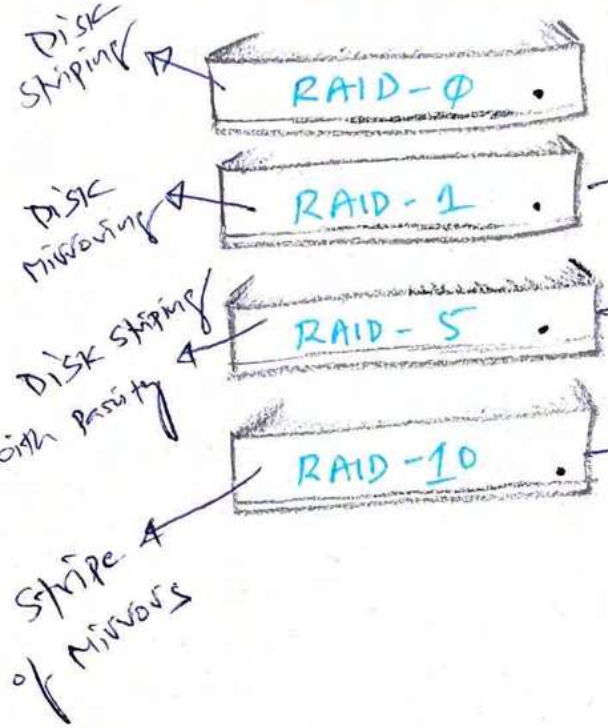
System Ability to return to previous state after an adverse event

Resilient server

Can run at least 10K after covid-19 injection



* Protecting Hard Drives



striping - 2 or more disk - Good performance but no fault Tol

Data Mirroring - 2 disk mirror data

striping with parity - slower - 3 or more dis

RAID 1+0 - at least four disks

↳ Continue to operate if one drive M1, M2 & M3 fails but if two drives in M1 fails - the entire array would fail.

Achieve fault Tol. + system resilience using

RAID Array

H/w RAID

$$$$

Reliable

Supports hot swapping

S/w RAID

$$

Need OS

No h/w required

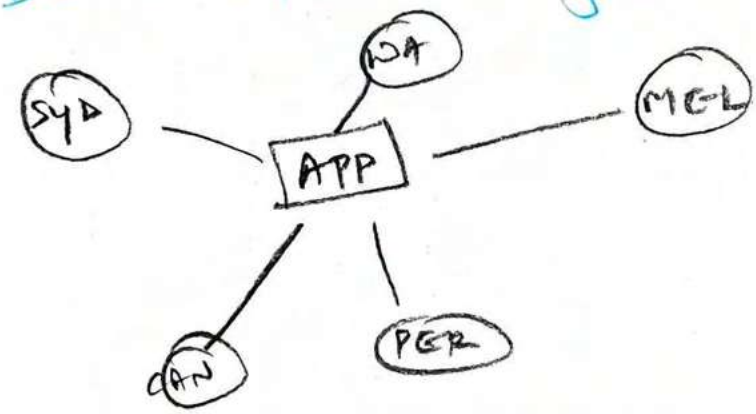
E.g RAID-5

* Protecting Servers

Use load Balancer → To address scalability
                  → Fault Tol.

IaaS providers auto scaling resources on as-needed basis.

Consider DC in different geographical locations



Failover cluster for availability.

consider Automatic Fault Tolerance for servers

↳ Automatic data replication b/w database servers.

* Protecting Power Sources

UPS

- Line-interactive UPS
- for short term

Generator

- For long term
- Needs fuel

* Trusted Recovery

↳ Ensures system is as secure as it was before the failure / crash.

A system can be designed to ~~fail~~ fail either in:

Fail-secure system

- default to this state in case of failure
- block all access

Fail-open system

- default to this state in case of failure
- grant all access

e.g. Firewall, example of Fail-secure with implicit deny philosophy, it will be secure but no availability. If (A) is important, fail firewall with fail-open, it will provide A but not security.

↳ Dilemma p.t.o

Fail-secure

Security but no availability.

Firewall Dilemma

Fail-open

Availability but no security

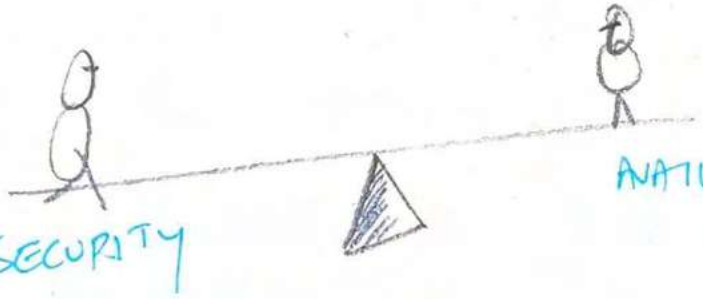
Electrical H/W locks

Fail-secure

- lock if power fails

Fail-safe

- unlock if power fails



---

2 Elements of implement a trusted Recovery process to Solution

Failure preparation

- System resilience
- Fault Tolerance
- Backup Solution

Process & System Recovery

- Reboot system into normal user A/C & don't allow unauthorised access
- Restore affected files & services

four types of trusted Recovery:

- Manual Recovery
- Automatic Recovery without Undue Loss
- Automated Recovery
- Functional Recovery

* Quality of Services — depend on some FACTORS

- Bandwidth
- Latency
- Interference
- Jitter
- Packet Loss

RECOVERY STRATEGY.

* Business Unit & Functional priorities

First — Identify & prioritize critical business functions that you want to restore after disaster & in what order.

BIA (Business Impact Assessment) can help.

BU - 1
Recover 50%.

BU - 2
Recover 20%.

BU - 3
Recover 10%.

Same exercise for all business function + process

output should be a checklist of items in priority order

- Risk
- cost
- MTTR (mean time to recover)
- MTO (max. tolerable outage)

BCP Planners assess these values for additional controls

* Crisis management

Results = PANIC Needs → Organised DR Plan

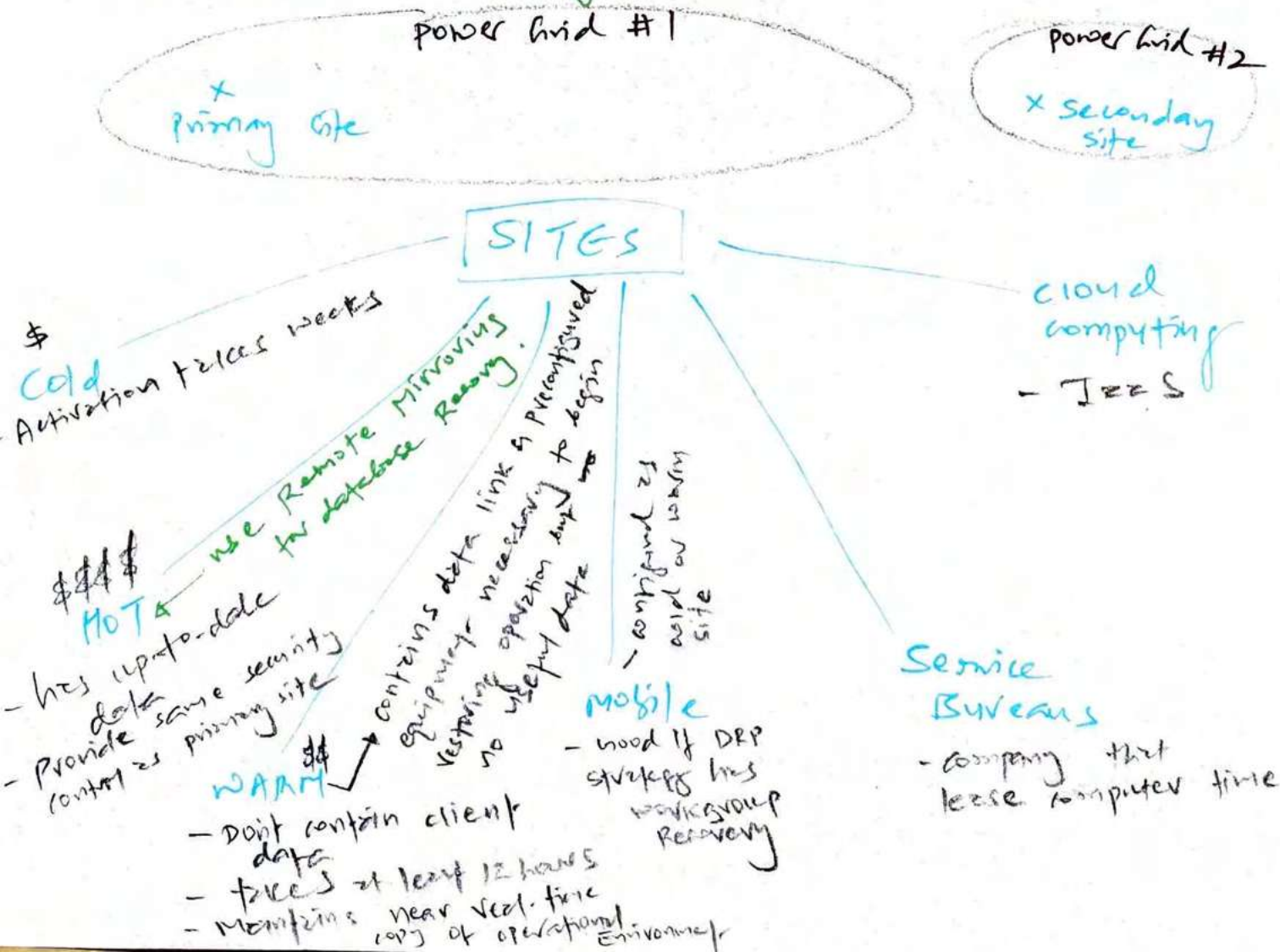
* Emergency communication

Communicate internally & outside the world

* Workgroup Recovery — Mobile site is excellent option

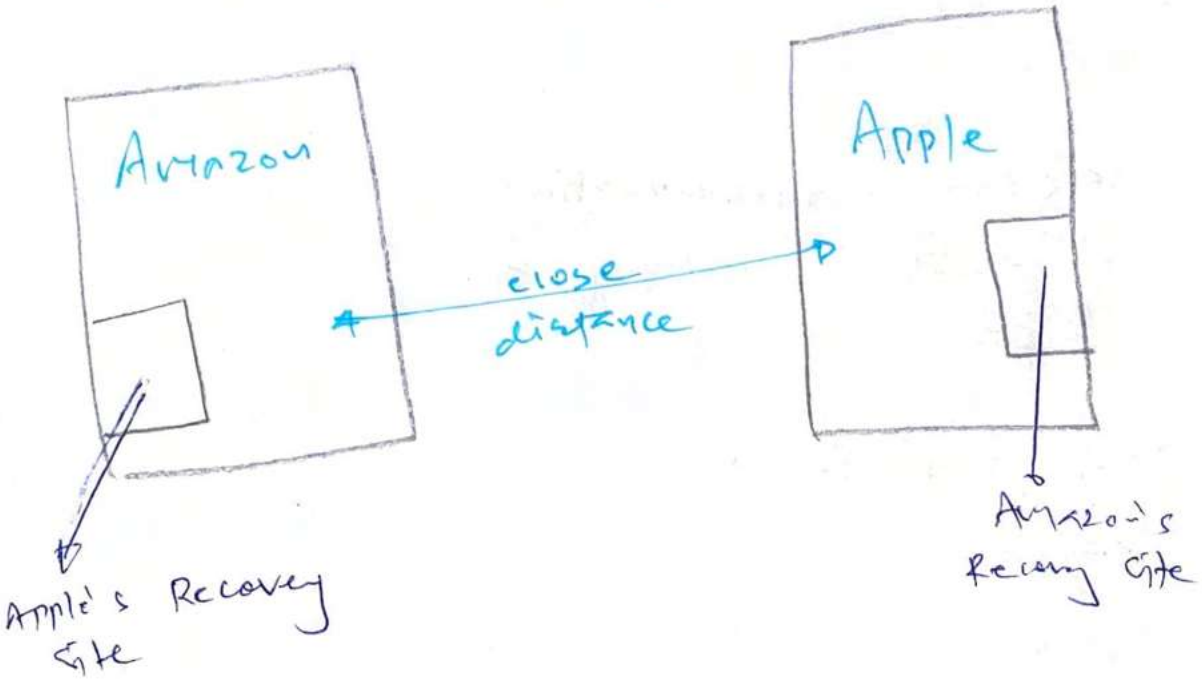
Seperate recovery facilities for different workgroups

* Alternate processing Sites



* Mutual Assistance Agreements (MAA)

└ Reciprocal Agreement



\+ → cost effective

\- → close proximity may be vulnerable from same threat
- └ Earthquake
- └ power outage

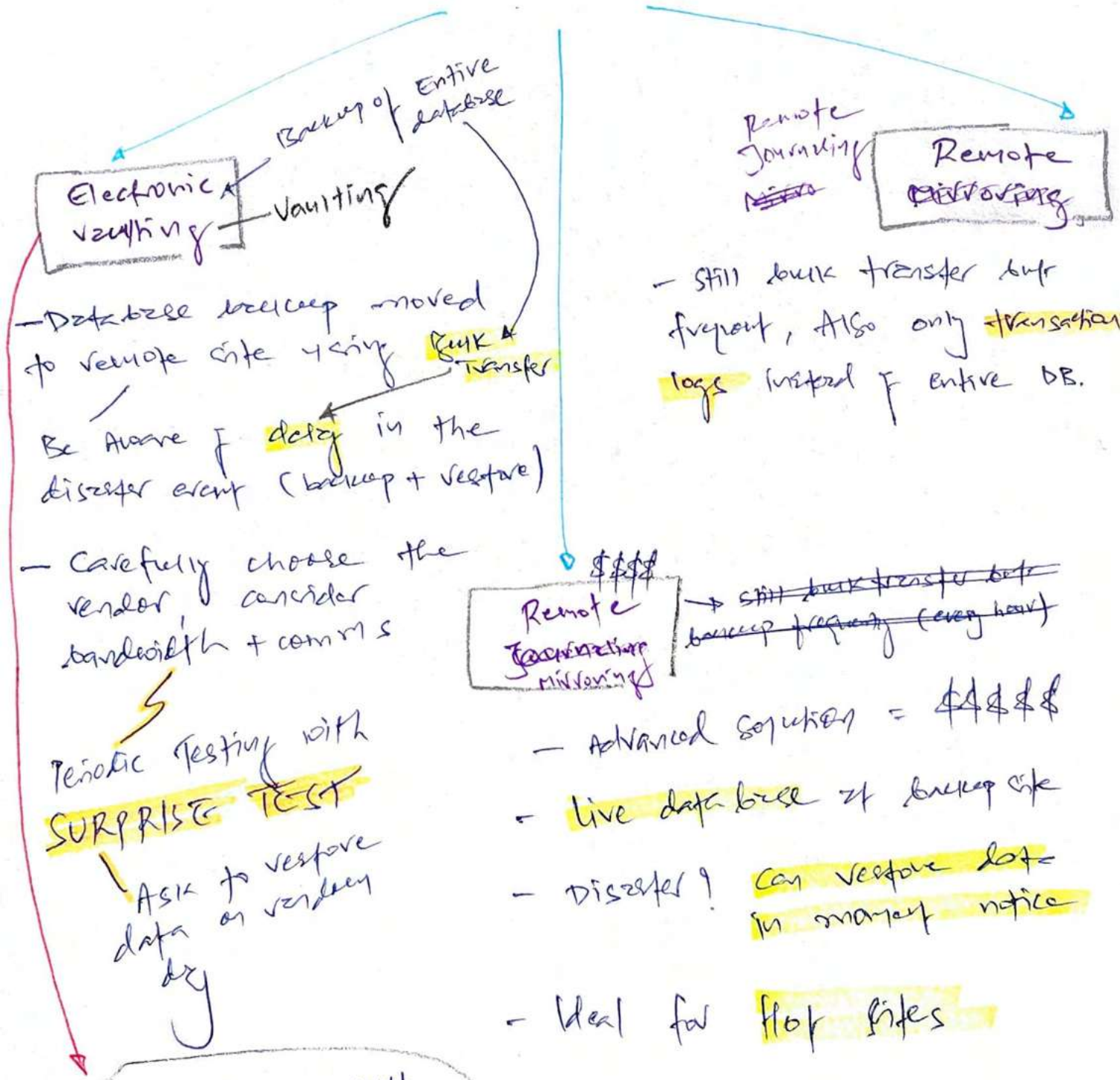
→ your data into other company! — confidentiality issue

Worst case
└ can't afford Alternate site! → MAA is the saviour

* Database Recovery

↳ crucial part of DRP

3 techniques for off site database copies



- Database backup moved to remote site using Bulk Transfer

Be aware of delay in the disaster event (backup + restore)

- Carefully choose the vendor, consider bandwidth + comms

Periodic Testing with SURPRISE TEST

Ask to restore data by vendor

- Still bulk transfer but frequent, Also only transaction logs instead of entire DB.

- Still bulk transfer but backup frequency (every hour)

- Advanced solution = $$$$$

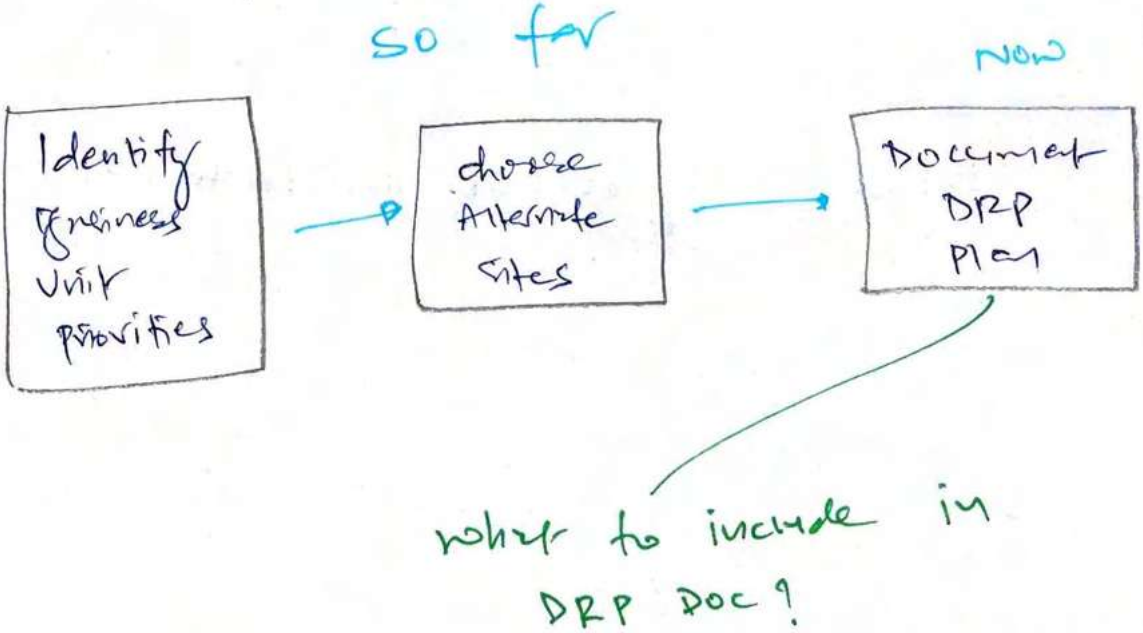
- Live database at backup site

- Disaster! Can restore data in minor notice

- Ideal for Hot sites

Note - Electronic vault introduces significant data loss. On the event of disaster, you will be able to recover information as of time of last vaulting operation.

RECOVERY PLAN DEVELOPMENT



- Executive summary - 10,000 ft of DRP plan
- Department specific plan
- Technical guides such as Backup Sq.
- checklist for individuals.
- Full copies of DRP to Recovery team members.
- And below sections

* Emergency Response = checklists

One principle in mind
=
Arrange checklist tasks in order of priority - most important task first

* Personnel and Communications

Key DRP members + Personnels who would perform DRP tasks.

should include Backup contact if primary not available

* Assessment

DRP Team's first task when Arrive on site → CIRCUIT - Assess the situation

* Backups and offsite storage

What's the Backup strategy for DRP?

Part of technical guide

BC + DRP's most crucial Element → Backup Strategy.

P.T.O = types of backups

3 Types of Backups:

Full Backups

- stores complete copy of data

Incremental Backups

- stores only those files that have been modified

faster to backup but it takes more time to restore

Differential Backups

- stores all files that have been modified since time of most recent backup

takes longer to backup than incremental but it's faster to restore

Difference is in time needed to restore the data

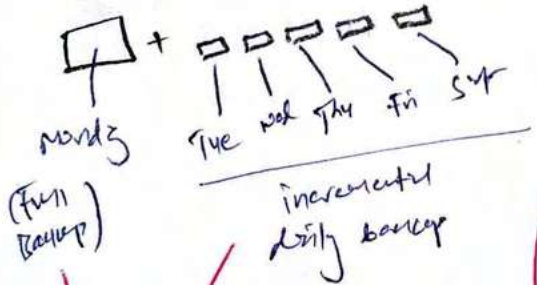
CORE CONCEPT

COMMON STRATEGY

- Full backup on weekend & incremental or differential backup on nightly basis

Strategy #1

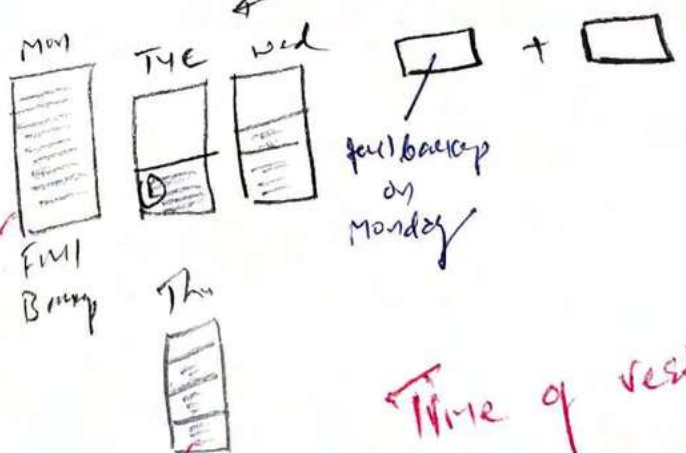
Full + incremental



Need all of them to restore, one if 'Tue' is corrupted!

Strategy #2

Full + Differential



Time of restore! only these two needed

Backup Type Formats

Physical characteristics

- Type of backup media
- old = less reliable

Rotation cycle

- Frequency of backup
- Retention length

Disk-to-disk Backup

↳ D2D backup strategy for DRP

↳ virtual tape libraries (VTL) : uses software to make disk storage appear as tapes to backup s/w.

↳ Consider geographical diversity

Backup best practise

- Night backup
- Deploy real-time backup → RAID cluster | server mirror img
- Test recovery process

Tape Rotation

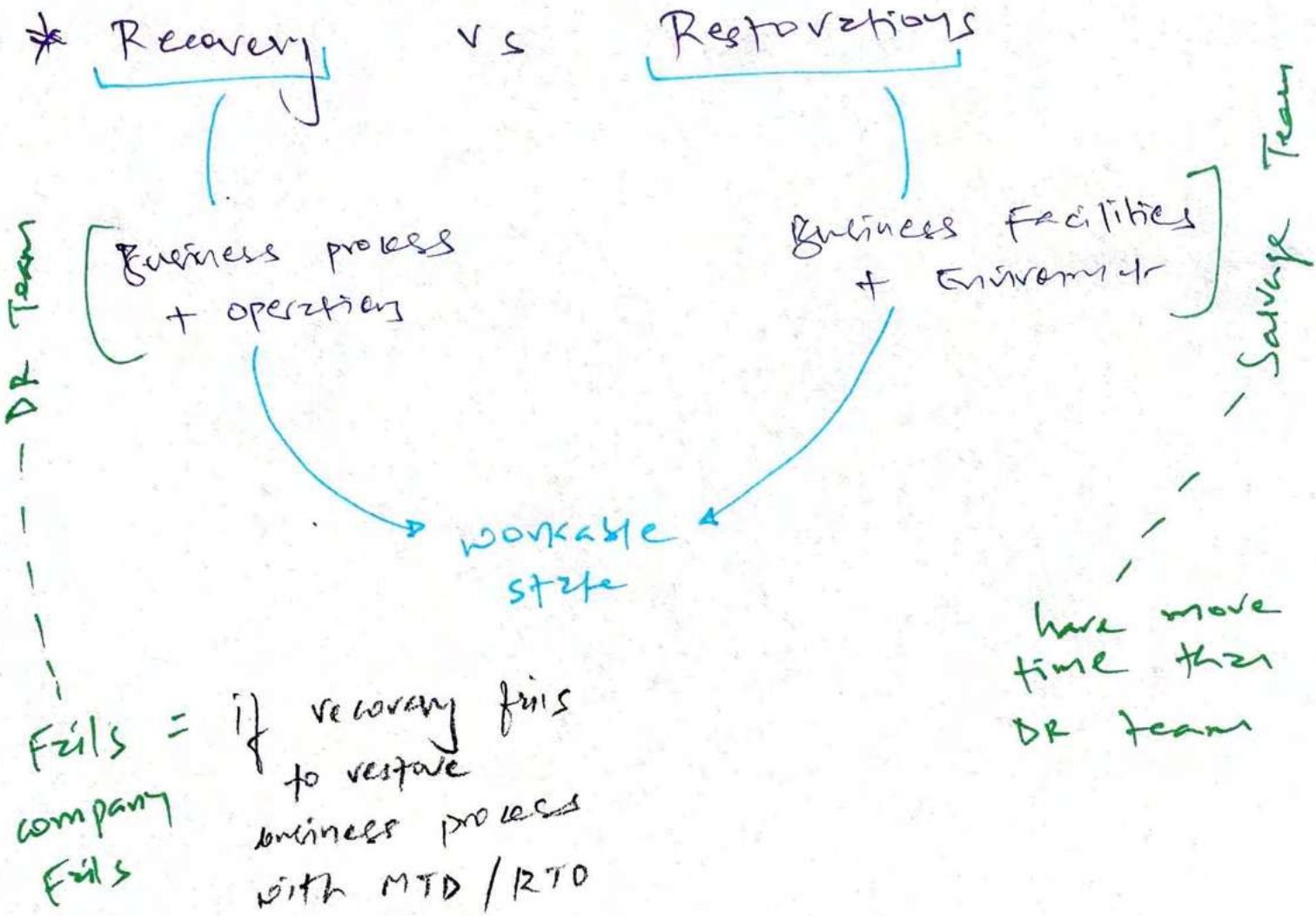
* Software Escrow Arrangements
  - Part of DRP plan

* External Communications
  - Media, Government authorities, vendors, suppliers, customers
  - comms to them = part of DRP.

* Utilities
  DRP to include contact details for Gas, Electricity, water ...

* Logistics & Supplies
  People may live at alternate site for extended period

*
  DRP to provision food, water & supplies for people


* Recovery
vs
Restorations
Business process + operations
Business Facilities + Environment
DR Team
Salvage Team
workable state
have more time than DR team
Fails = if recovery fails to restore business process with MTD / RTO
company Fails

TESTING & MAINTANANCE → p.t.o context

TRAINING, AWARENESS & DOCUMENTATION

Read-Through Test

- Send DRP to team member for review

Structural Walk-Through

- Table Top Exercise
- DRP team gather in room for discuss scenario

Simulation Test

- DRP team presented with scenario & asked to develop appropriate response

Parallel Test

- Personnel to go to site alternate site to activate process, pretend that main site is down

Full-interruption Test

- Actually shut-down primary site & activate DR site
- This is risky
- Most don't like this

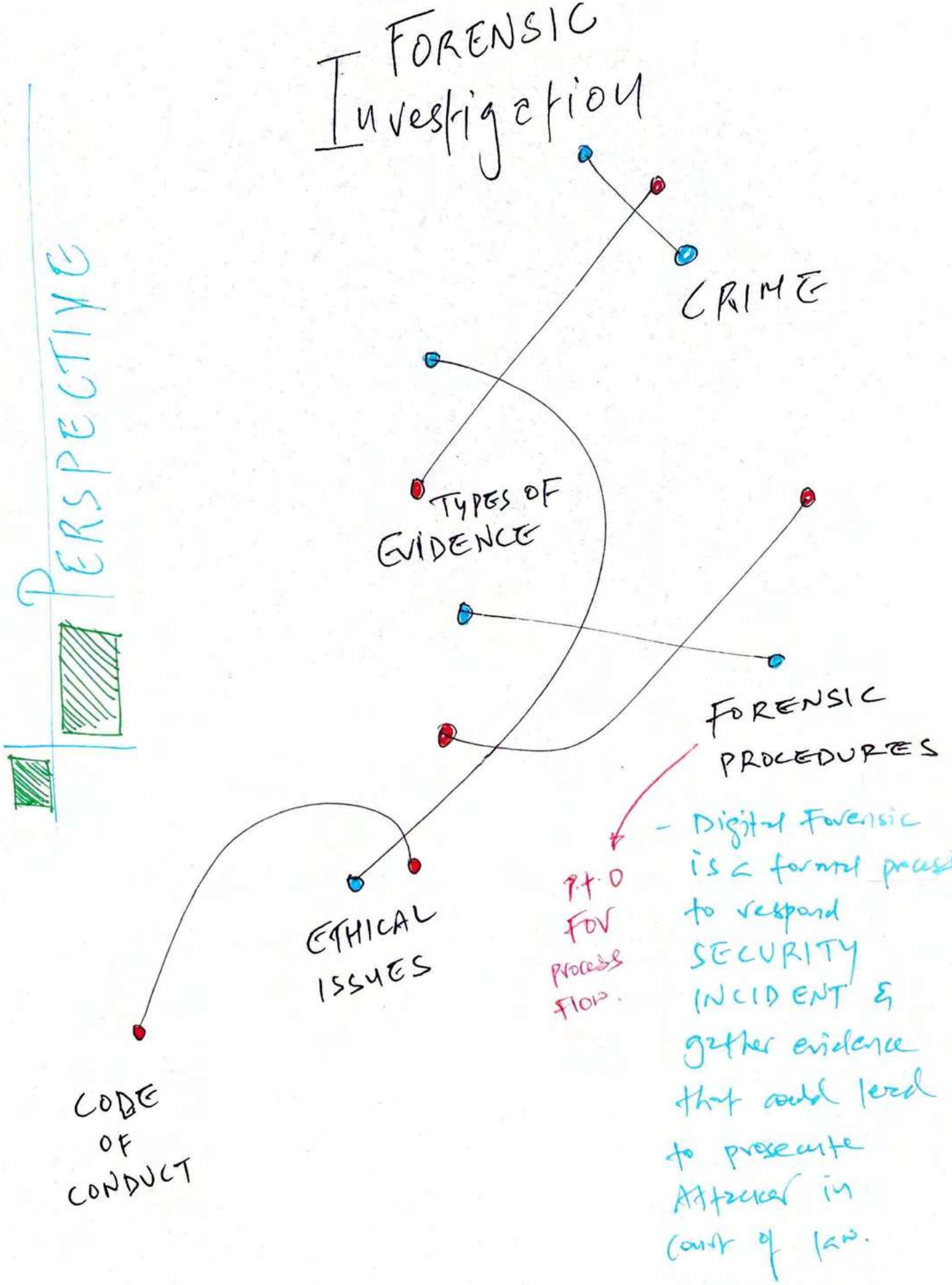
Maintenance

- DRP = living document

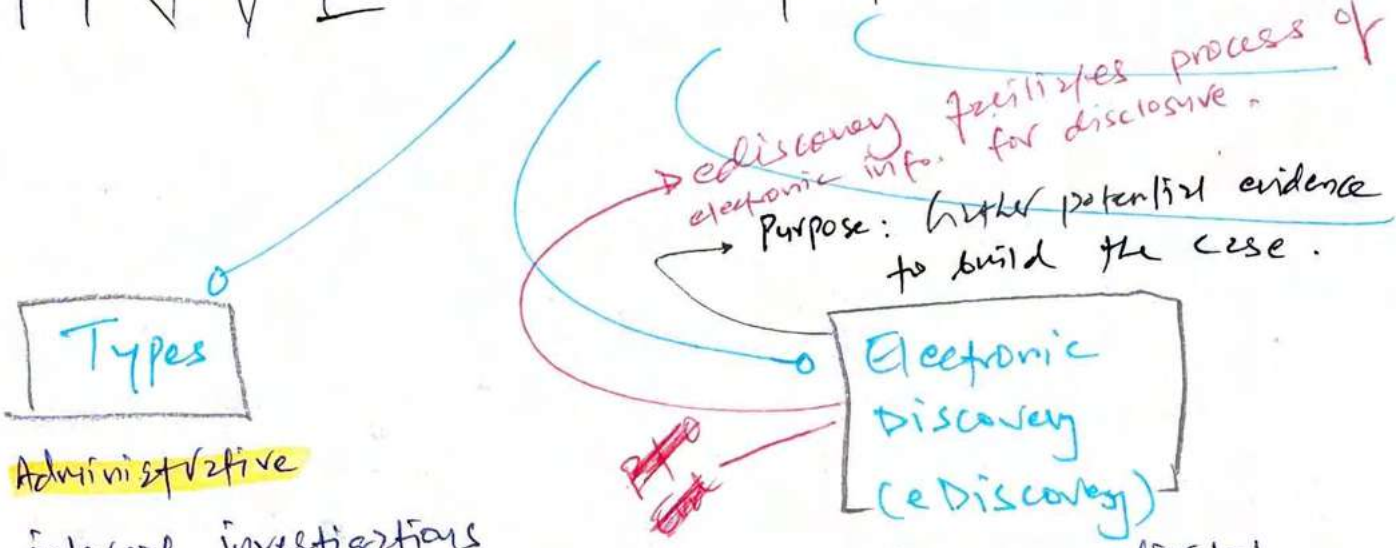
Any changes in organization must reflect DRP

- DR plan = should refer organization BC plan

19. INVESTIGATIONS AND ETHICS



INVESTIGATIONS



1. **Administrative**
   - internal investigations
   - To Resolve operational issue
   - Not much evidence required, Performs root cause Analysis

2. **Criminal**
   - strict evidence collection + Preservation process
   - violation of criminal law

3. **Civil**
   - Involves internal employee + outside consultants
   - Involves civil court to resolve dispute b/w two parties
   - Not intense evidence collection

4. **Regulatory**
   - Government agencies
   - PCI DSS ! or pay fine $$$

- To preserve digital evidence, 9 steps
  - 1 → Info. Governance
  - 2 → Identification
  - 3 → preservation
  - 4 → Collection
  - 5 → Processing
  - 6 → Review
  - 7 → Analysis
  - 8 → production
  - 9 → presentation
    - present in court + other parties

Evidence

Admissible Evidence has 3 requirements

- Relevant
- material (related to case)
- competent (obtain legally)

3 Types of Evidence

1. **Real Evidence / Object Evidence**

2. **Documentary Evidence**
   - written items such as computer logs
   - Best Evidence Rule
   - Parol Evidence Rule

3. **Testimonial Evidence**
   - Testimony of witness
     - Direct Evidence
     - Expert opinion
     - Hearsay Evidence

if logs are not authenticated, are hearsay Evidence = contraband

P.t.o End

Investigation Process

P.t.o

Evidence Collection & Forensic procedure

Don't play with original evidence, investigate with copy

Forensic Analysis

P.t.o End

- Media Analysis
- Network Analysis
- Software Analysis
- Hardware/ Embedded Device Analysis

Investigation process — P.t. 0 End for Entire process

* First build Awesome Analyst Team

1. Gathering Evidence (collecting Evidence)
   - is important but how to confiscate is more important

3 Alternatives for evidence gathering

- Person who owns evidence voluntarily surrenders it.
- Get court to issue subpoena / court order
- Last option based on जरूरी — surgical strike — search warrant

This leads to surrendered evidence

ANOTHER STEP — Add in the policy

Add to provide consent to search for evidence for new employees as part of Employment agreement

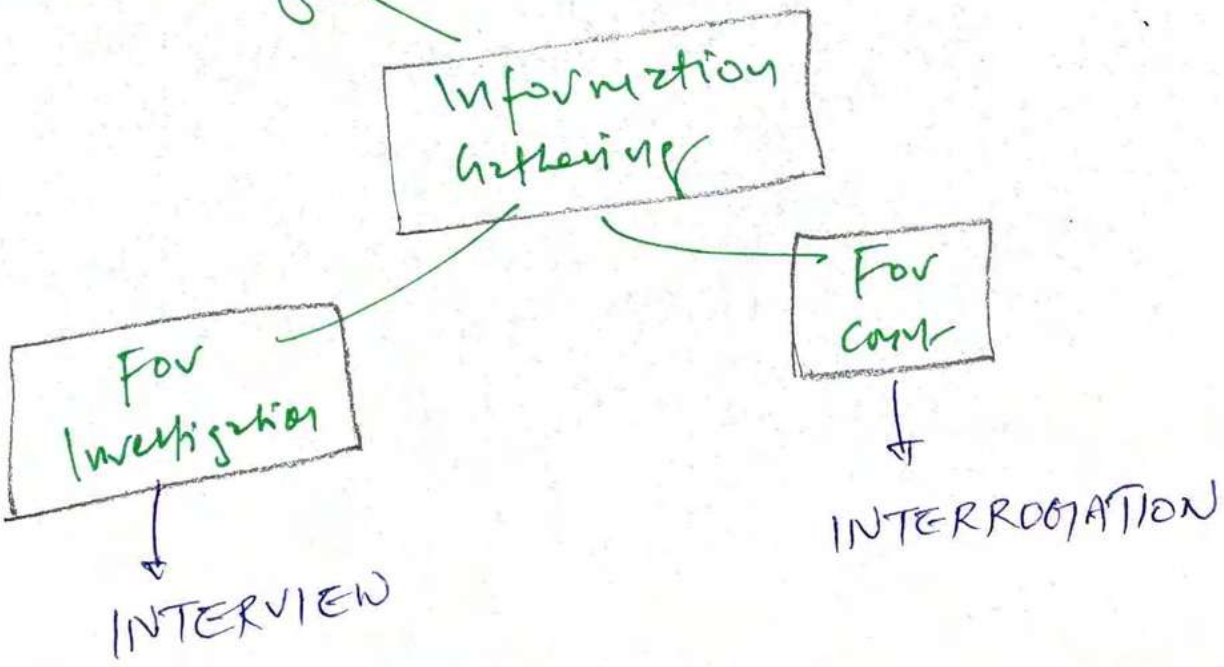
- Calling In Law Enforcement
  - 2 factors company may not call FBI
    - Public Embarrassment
    - Investigation may reveal other wrongdoings

Conducting the Investigations

FBI Alternatives + Tips

- Don't investigate on actual compromised system
- Hire Private Investigator
- Don't Hack back to avenge. Might hurt innocent 3rd parties.

Interviewing Individuals



- Always contact attorney before conducting any interviews.

Data Integrity and Retention

- maintain the integrity of the evidences and integrity of the data before you collect from the crime scene

how? P-t-O

↳ Simple Archive Policy : Ensures key evidence is available upon demand no matter how long ago incident was occured.

↳ Protect integrity of log files : Remote logging + Use of Digital Signatures

All system send log records to secure centralised server

↳ Reporting & Documenting Investigations

Start of Investigation

Administrative / internal — can turn into criminal investigation — Be prepared

Prepare formal documentation.

Establish relation with legal corporate team + law enforcement agencies

Find single contact to liaise with law enforcement

Easy for all "go-to" updates for one person

Predesignated Contact to work with law enforcement

MAJOR CATAGORIES OF COMPUTER CRIME

Understand the attack + attacker

helps → How to protect & Recover

helps → What evidences to look for after the attack

(1) Military & Intelligence Attacks

Goal: To obtain restricted / secret information

How To protect: → stringent perimeter security
→ Internal controls

Evidence: Usually no evidence to collect as Attackers are pro-level

(2) Business Attacks

Goal: To illegally obtain organization's confidential information

How To protect: Risk mgmt + controls

Corporate / Industrial Espionage

MOVIE NAME

③ Financial Attacks ← Shoplifting
← Burglary

Goal : To obtain money

[$1000 ← Newbie
$1000000 ← Sophisticated Attacker

④ Terrorist Attacks

Goal: To disrupt normal life & instill fear

JOKER

Future of Attack — physical Attack + computerized Attack } simultaneously

Prevent: 24x7 monitoring

⑤ Grudge Attacks

Goal: To damage person / organization reputation + loss of information

FIRED EMPLOYEE

Protect: Security policy — disable all access of terminated Employees

perform vul. Assessment for "Back Doors"

(6) Thrill Attacks

How: To have Fun

By Script Kiddies: Attackers use other people's programs/scripts to launch the attack.

Most. consequence of Attack: Service interruption (most common)

E.g: Website defacement
Attacker replace legitimate webpage with other one

Rise of Hactivist — Hacker + Activist — political motivation with thrill of hacking

---

FORENSIC DISK CONTROLLER FUNCTIONS

What it is?

- Write blocking
- Intercepts write commands sent to device
- Prevent them from modifying data on the device

- It's a hardware write-block device made for the purpose of gaining read-only access to computer harddrive without the risk of damaging the drive's content.

ETHICS

Two code of Ethics

- $(ISC)^2$ code of Ethics
- Ethics and the Internet

(1) Protect society, the common good, necessary public trust, and confidence and infrastructure.
- public safety

(2) Act honorably, honestly, justly, responsibly, and legally.
- Duties to principals (संस्थान, नियोक्ता, ग्राहक)

(3) Provide diligent and competent service to principals.
- Duties to Individual

(4) Advance and protect the profession.
- Duties to profession.

Forensic Analysis

Media Analysis

- Identification & extraction of information from storage media.
  - magnetic media (hard drive)
  - optical media
  - memory
- Techniques → Recovery of deleted files from unallocated sectors from physical disk
  - Static Analysis of forensic images of storage media

Network Analysis

- Activity that took place over network during a security incident.
  - IPS
  - Netflow
  - packet capture
  - logs from firewall

E.g. Reviewing logs from web server is network analysis.

Software Analysis

- Forensic look for SW / Application source code for
  - malicious code
  - Backdoor activity
  - logic bomb
  - or various database file for SQL injection
  - Review privilege Access & other Application Attacks

Hardware / Embedded Device Analysis

- Need experts who has specialized knowledge in
  - memory
  - OS
  - storage

4th Amendment - Prevents law enforcement agencies from searching home/facility without consent or probable cause

1st Amendment - Protection related to freedom of speech

5th Amendment - Ensures no person will require to serve as witness against themselves.

15th Amendment - Protects the voting rights of citizen.

Testimonial Evidence

Direct Evidence
- when witness testify about their direct observations

Expert opinion
- Allows individuals to offer their opinions based on facts + personal expert knowledge

Hearsay Evidence
- Testimonial evidence should not be hearsay
- Someone told me about - but outside the court
- E.g. logs that are not maintained by server is hearsay evidence

Real Evidence → tangible items

Documentary Evidence → consists of written records

ISO/IEC 27037 Guidelines for Digital Evidence

Digital Forensic Process

4 steps

1. **Identification** of Evidence — Maintaining integrity is critical before collecting evidence & after that we present in ~~court~~ court

2. ~~collection~~ **collection** of Evidence
   - labling evidence with date, time, location
   - chain of custody (chain of evidence) is crucial

3. **Acquisition** of Evidence
   - creating forensic image of digital data for examination (primary image & working image)
     - primary image → stored in library
     - working image → For Analysis
   - Acquisition also means to collect evidence from volatile sources such as RAM, cache, temp file system & special disk sectors.

~~3~~ Analysis of Evidence - - - - - - - - -

4. **Preservation** — Already: chain of custody & use of hash to maintain integrity
   - Ensuring minimal authorised personnel
   - has access to digital evidence.
     - ↳ implement MofN control

The Forensic Investigation Process.

1. Identification of Evidence
   - Identify your assets that were affected.

2. Preservation of Evidence
   - chain of custody from time of seize to time when present in court
   - To maintain the integrity throughout forensic lifecycle

3. Collection - Taking control legally
   - Gathering Evidence
     - volunteer
     - court issue subpoena
     - search warrant
     - corporate policy
   - Admissible evidence
     - Relevant
     - Material
     - Competent

4. Examination - Time consuming
   - Document findings
   - Tools of forensic
   - create forensic image
     - primary image
     - working image — Examine with this copy

Should be part of preservation

5. Analysis — find the root cause
   - Analysis types
     - Media
     - Network
     - Software
     - Hardware
   - what root cause does the evidence point to?

6. Presentation (Reporting)
   - Present evidence in court, may need Expert to testify
   - Evidence Types
     - ~~Direct~~ Real
     - Documentary
     - Testimonial
       - Direct
       - Expert opinion
       - Hearsay

7. Decision
   - Are they guilty or not?

DOMAIN 8

CH: 20 SOFTWARE DEVELOPMENT SECURITY

Custom s/w development to achieve unique business objectives

→ security Vulnerabilities

Malicious code

Backdoors

Attackers

Rely on 3rd party code + libraries

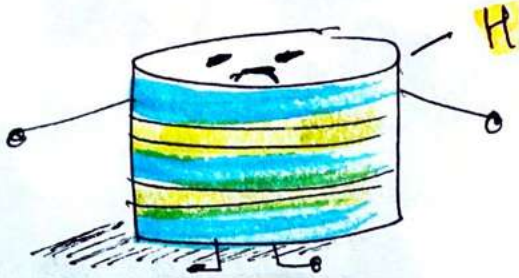
PERSPECTIVE →

Inject Security control into SDLC - s/w Development life cycle.

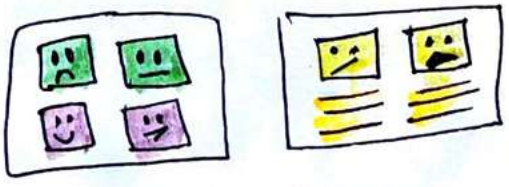
BE AWARE - WHOM WE NEED PROTECTION FROM?

Malicious code

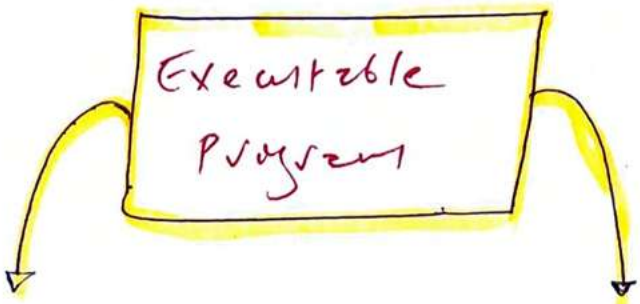
Database Vulnerabilities



Application Development flaws



* S/W Development



Compile

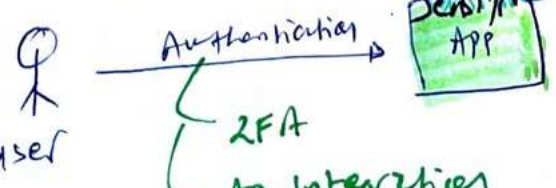
- Code convert into executable file then distribute to end users — not the source code
- * Programmer can embed malicious code
- C, JAVA

Interprete

- Distribute source code to end users
- * User can review code & insert malicious one
- Python, Javascript

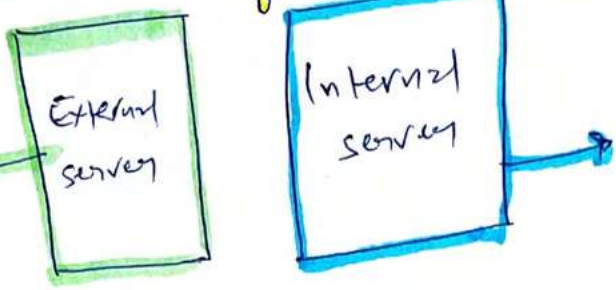
Avoiding & mitigating system failure with some methods.

1. Input validation (from user) ← occurs on server side of transaction
   - DOB <integer>
   - state <three word etc>
   - ⇓ LIMIT CHECK + ESCAPING INPUT
2. Authentication & Session mgmt
   - Session tokens



Level of Authentication ∝ sensitivity of application

3 ↳ Error Handling



Debug report to Attackers = bad idea

detailed debugging report for developers = good idea

4 ↳ Logging = SIEM = stack driver

5 ↳ Fail-secure & Fail-open = 2 choices of planning system failure

... Famous BSOD

This is better for security reasons

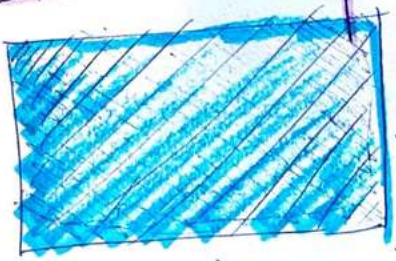
Enable full security or disable all to diagnose problem to restore system

Bypass security controls.

BLUE SCREEN

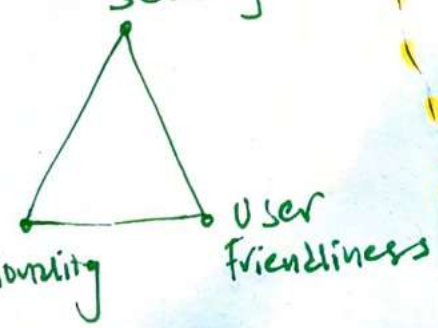
(Fail-secure response)

Blue screen of Death (BSOD) = STOP Error



- Application gaining direct access to H/W
- Attempt to bypass security check
- Memory interference b/w two process

→ often we Disable security in s/w for easy installation



* Software Development life cycle (SDLC)

7 Core activities for secure system Development:

1. Conceptual Definition
   - project purpose & system requirements
2. Functional Requirement Determination
   - Input
   - Behavior
   - Output
   - For all system requirements
3. Control specification Development
   - Security controls
     - Access controls for authorised users
     - maintain confidentiality & data using Encryption + Data protection methods
     - Address Availability & Fault-tolerance
     - Enforce Audit + Accountability or detective mechanisms for illegal activity.
4. Design Review
   - Based on 3 & 2
5. Code Review walk-through
   - check for problems in logic flaw / design / security flaw.
6. User Acceptance Testing (UAT)
   - All sort of user testing before code moves to deployment / prod.
7. Maintenance & change mgmt.
   - Deploy

* lifecycle models

Gantt chart & PERT

S/W capability maturity model

(SW-CMM) idea = Quality of S/W depends on quality of development process.

- 5 stages (P.T.O)

Agile model

- Supports Devops with continuous delivery + deployment

IDEAL model

- Implements many SW-CMM attributes

Spiral model

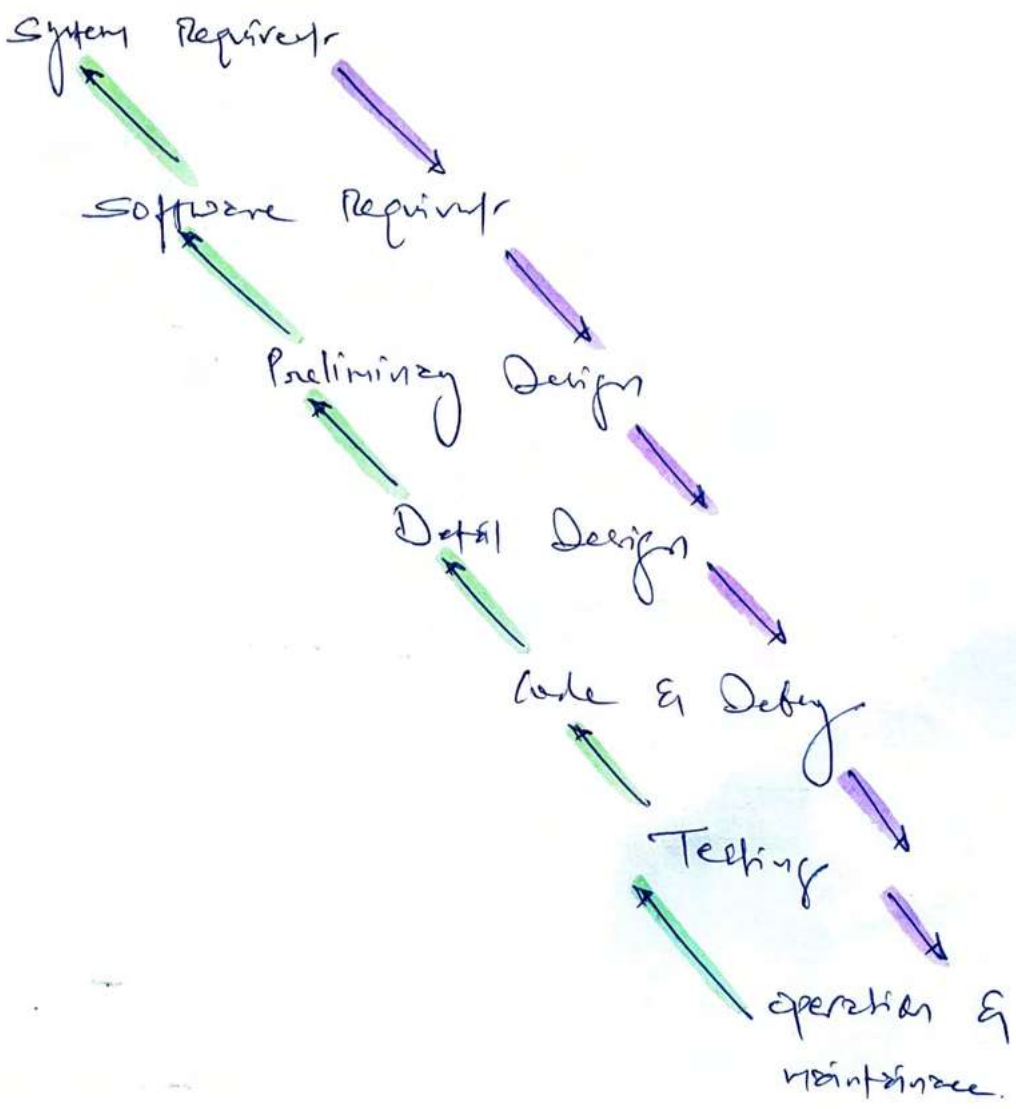
- Multiple iterations of waterfall model
- Each loop of spiral results in the development of new system

Waterfall model

- System development lifecycle as a series of iterative activities.

→ Developer can sit back & watch till five vises in production.

Waterfall Model



IDEAL Model

1. Initiating - Business reasons to change are outlined
2. Diagnosing - Analysis of current state of organization + recommendations
3. Establishing - Develope specific plan based on recommendation & change
4. Acting - Stop "talking the talk" start "walk the walk"
5. Learning - Feedback → Continuous improvement

Software Capability Maturity Model (SW-CMM)

- Quality of s/w & Quality of development process.

5 stages.

Level 1 : Initial

- Little to no defined s/w development process

Level 2 : Repeatable

- Basic lifecycle mgmt process are introduced, such as reuse of code.

Level 3 : Defined

- Developer operate according to set of formal, documented s/w development process.

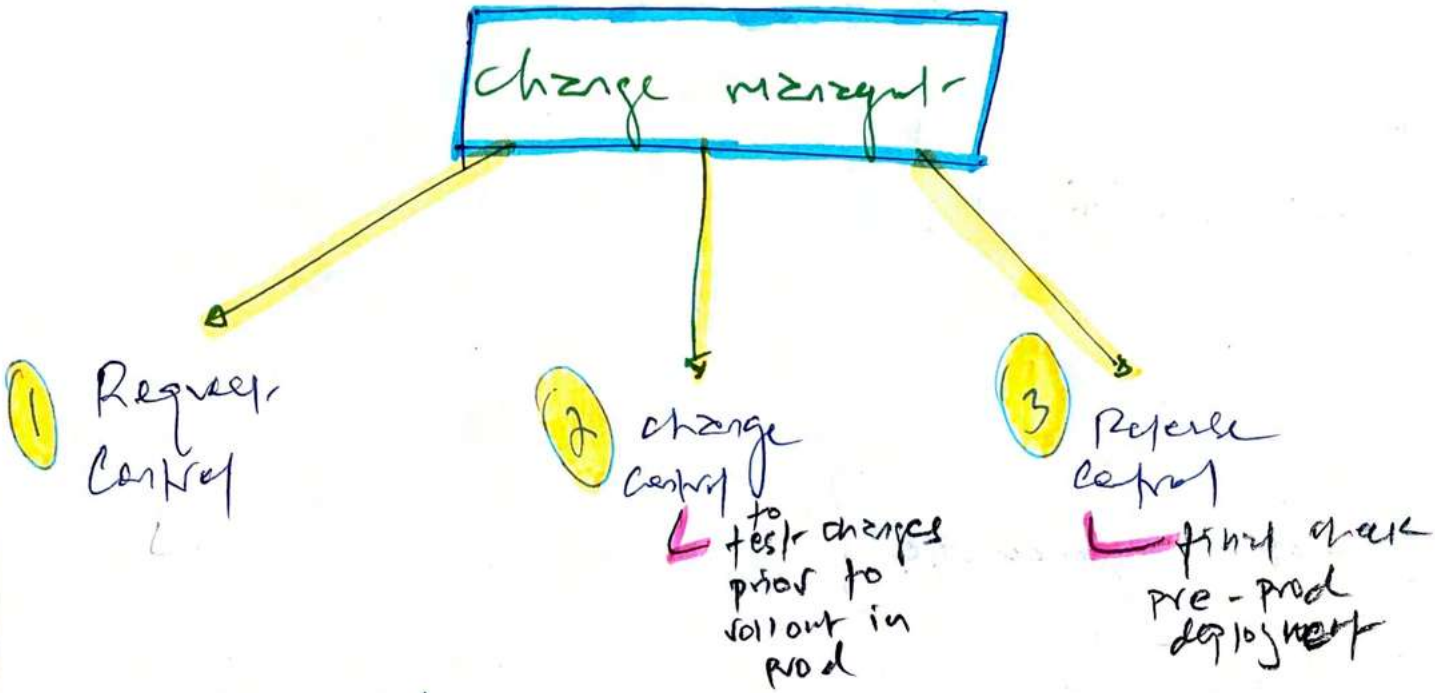
Level 4 : Managed

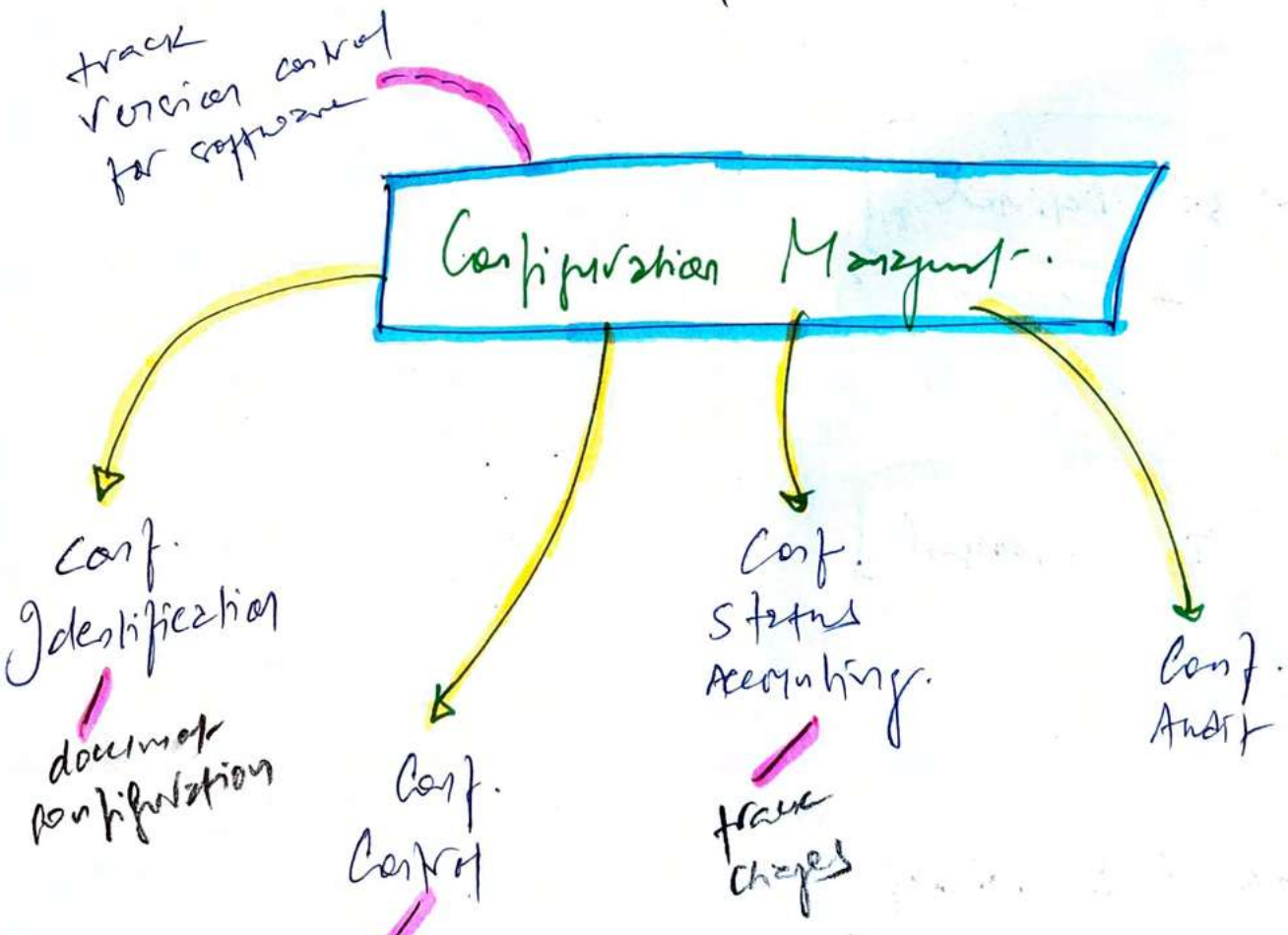
- Quantitive measures are utilized to gain detailed understanding of development process.

Level 5 : Optimizing

- Process for continuous improvement

* Change & Configuration Mangemt.

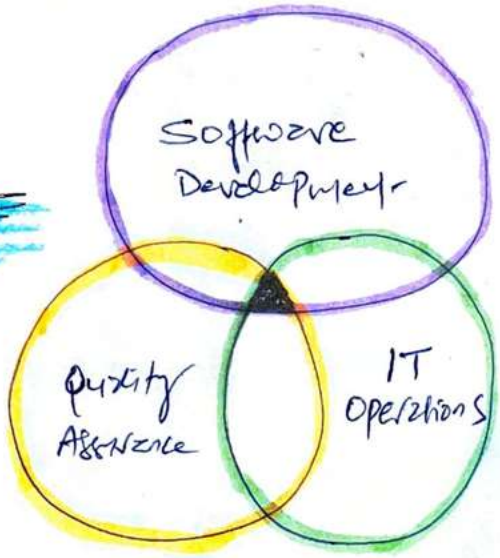




* DevOps Approach --- Aligned --- Agile Development Approach

Create code
Test code
Deploy code

→ 3 function into one operational model



Information security is NOT part of DevOps.

API

API Keys = To identify Project / Application (nothing to do with user)

Heroku vars

Don't put in public repo

Project Identification

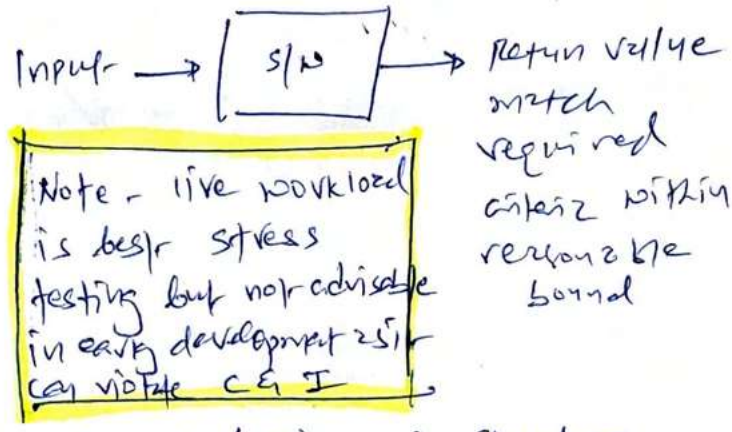
project authentication

User → Authenticate

→ Authorize

Software Testing

Perform a test called Reasonable check



3 Methods

i) White-box testing
- test internal code + logic + structure

ii) Black-box testing (E.g Fuzz Testing)
- From user perspective (input + output scenarios)
- they don't have access to internal code

iii) Gray-box testing
- Hybrid : popular for s/w validation

Application Security

Static testing (SAST)
- For pre-prod / source code
- Inform running app. or source code

Dynamic testing (DAST)
- For runtime / prod
- Web Application Testing: E.g SQL injection for web app + XSS

Software Acquisition

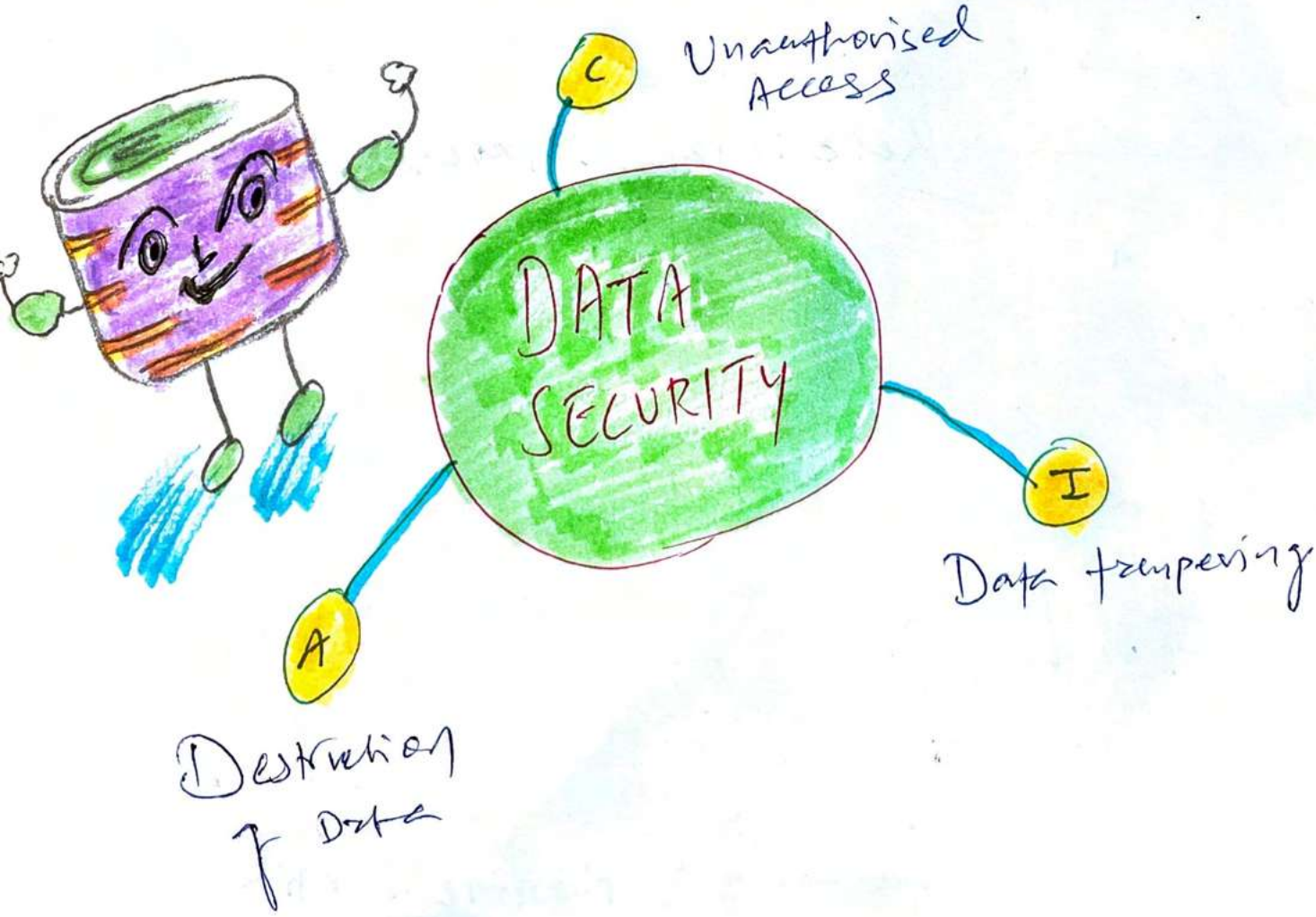
IaaS

- Physical / virtual
  Exchange server
* in-house security

SaaS

- Gmail
* Monitor vendor's security

DATABASE & DATA WAREHOUSING



Database Architecture

1-M Hierarchical Database

- organization chart
- one database
- one to many relationship.

M-2-M Distributed Database

- data stored in more than one database but they are logically connected.
- may-to-may relationship

cardinality = Rows
Degree = Columns

Relational Database

Candidate Keys

ID	Email	mobile

Primary Keys

selected as primary candidate → ID

Foreign Keys

Referential Integrity → mobile

Database Table

compliance with normal Form → Normalization (pt. of 2)

- 1NF
- 2NF
- 3NF

Database language → SQL

SQL → 2 components

DDL - Data Definition Language

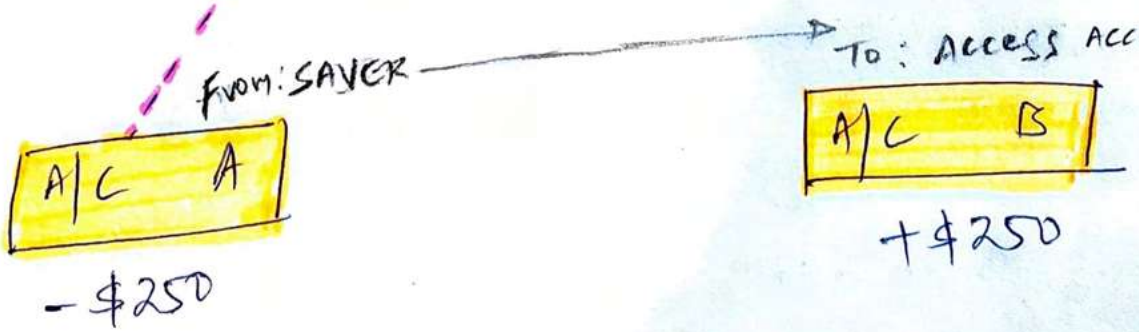
- Allows creation & modification of database structure (schema)

DML - Data Manipulation Language.

- Allows users to interact with data contained within that schema.

Database Transactions

Implicit and Explicit use of transaction → Ensures → DATA Integrity



*Adding & removing fund executed as one transaction, not seperate.

Database transactions 4 characteristics

ACID

Atomicity

transaction = All or nothing

(A) Durability

Once data is committed to database = it must be **Preserved**

Using Backups, transaction logs

(I) Consistency

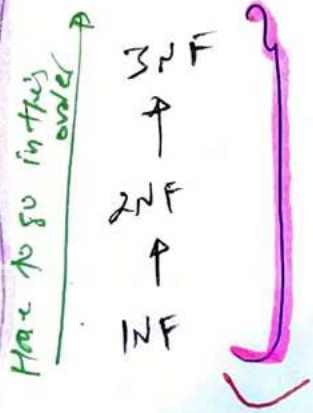
All transaction use = Consistent / updated data

(I) Isolation

logs ✓ inventory ✓

Used to organize data in relational database.

Database Normalization — Process of bringing database into compliance with various forms



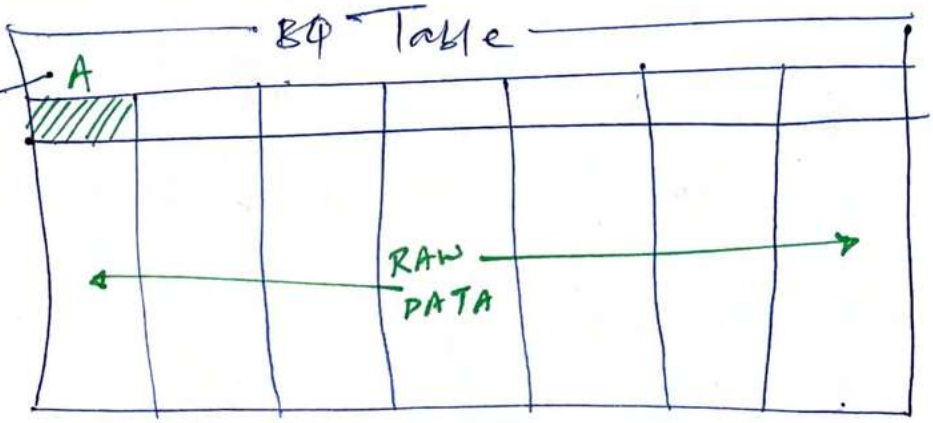
These forms adds requirements to reduce redundancy in tables, eliminating misplaced data in tables, & perform other housekeeping tasks.

DATABASE SECURITY

(From DB Admin perspective)

→ Data classification as a go-to-start security

BUT



only access to column A rather than whole table

=

DATABASE VIEW

1 ---- multilevel security in Database

- Views are stored as SQL commands rather than tables of data.
- OR query

(Edit control) CONCURRENCY

2 ---- Preventive security mechanism to protect Integrity & Availability.

- Two different processes update same database and unaware about each other's activity.

Without concurrency

- Lost updates
- Dirty Reads

Lock feature (Similar to Palo Alto's COMMIT)

- Process reads a record from transaction that successfully did not commit (SQL)

When multiple security required for database, it's better to keep requirement separate. Mixing classification levels / need-to-know requirement is known as Database Contamination

Semantic Integrity

3 - To ensure user's action don't violet structural rules.

- Security feature for DBMS
- Checks all stored data types are within valid domain range, ensures the logical values exists

Employ time & date stamps

4 To maintain data integrity & availability.

Granular control (Using OBJECTS)

6 5

Content-dependent access

Based on content or payload of object being accessed

relates

Context-dependent access control

How each object / field relate to overall activity / communication

Cell suppression

Hide individual database field / cell.

Polyinstantiation

(Prevents unauthorised user to view classified info)

P.I. end

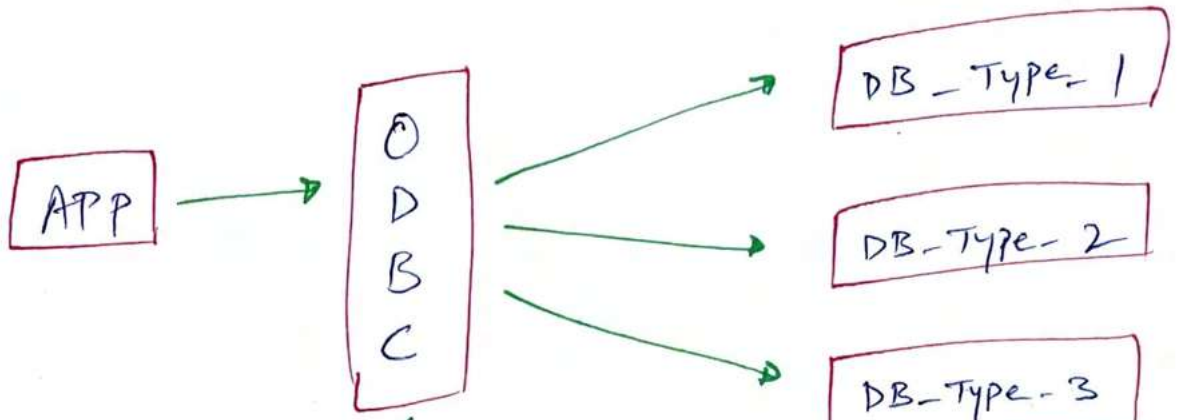
7

- Two rows, same primary keys, different classification levels.

Ship46 ---- top secret = undercover

1 2 3 ---- secret = normal routine

Other ships



as = Proxy

Open database connectivity.

Database

SQL

NoSQL = free

Use models other than relational models to store data.

Types

1. Key/value stores

- 1- Dave
- 2- Kyoto
- 3- Rocks
- 4- Always

2. Graph Database

3. Document stores.

- XML
- JSON

Data Storage

Not just security of data, consider types of storage too ---

1) Primary storage = RAM = Volatile / Real
   - CPU

2) Secondary storage = DVD / USB (Non Volatile)

3) Virtual Memory = simulate primary storage

4) Virtual storage = simulate secondary storage
   - E.g RAM DISK

5) Random Access = as can reqest content from any point within media
   Storage
   - RAM, Harddrive

6) Sequential Access storage = requires scanning through entire media to reach specific address
   - Magnetic tape

7) Volatile storage = RAM (System CPU)
   - Power-off = data gone

8) Non-volatile storage = DVD / USB
   - Power-off doesn't matter

How insecure is data in Database!

Storage threats

Unauthorised Access

(C) Confidentiality

Controls

- Encrypt data
- Store key in secure vault
- Least privilege / RBAC
- Monitoring
- Classification of data + Asset
- ★ Ensure data on higher classification level is not readable at lower classification level.

Covert channel Attacks

Transmission of sensitive data b/w classification levels, through direct / indirect manipulation of shared media.

SPECTRE & MELTDOWN

* Knowledge Based Systems - AI

Expert Systems

= No Emotions for investment decisions.

① Knowledge Base
- Expert human knowledge codify into series of if / then statements

② Inference Engine
- Analyse ① Knowledge Base & agsive or appropriate decision.

10 Thriller Films you might like

watch "Pi"

Extension → Neural Network

Neural Networks

- Attempt to imitate biological logical reasoning process of human mind.
- Extension of machine learning / deep learning / cognitive system

= Superior than AI

- Delta learning rule: neural networks are able to learn from experience.

(DEEP) Machine Learning

Extension → Neural Network

Model to detect malicious logins

Supervised Learning (labeled data)

model Trains → prediction

Unsupervised Learning (Unlabled data)

independent model based on their own learning.

Analyst learn malicious login attempts & build a model

REMEMBER

IDEAL model & SW-CMM model

"I ... I — . Dr. Ed ... Am Low)"

IDEAL	SW-CMM
Initial	Initial
Diagnosing	Repeatable
Establishing	Defined
Acting	Managed
Learning	Optimized

SDLC

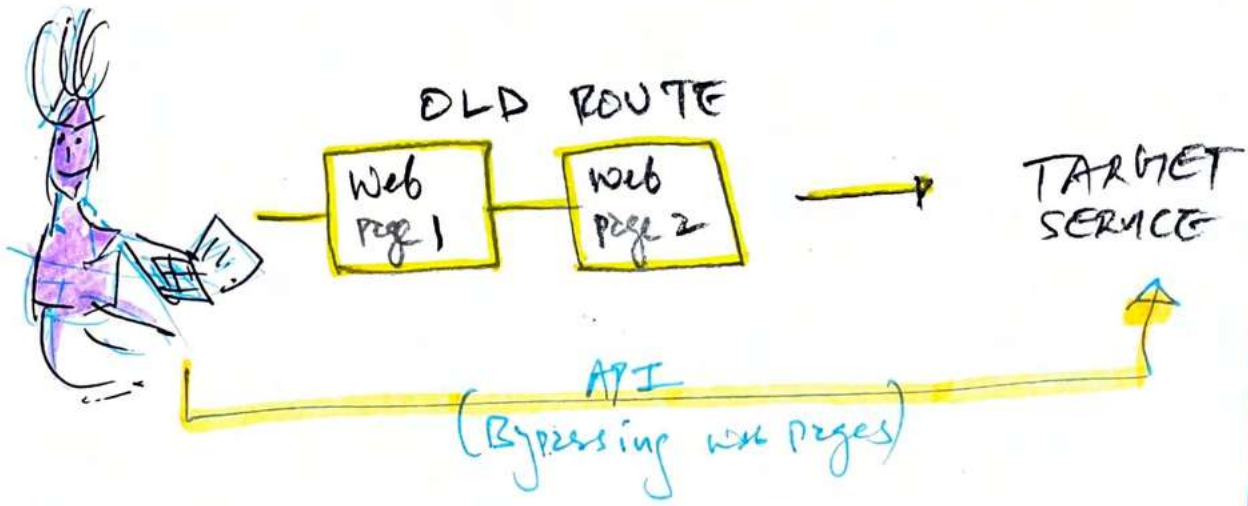
C F C D C S M

- Conceptual definition
- Function req. — Input, Behavioral, Output
- Control specification development
- Design Review
- Coding Review
- System test Review
- Maintenance & chg. mgmt.

Waterfall

SR^2 PD DD C T O

- System requirement
- Software requirement
- Preliminary Design
- Detailed Design
- Code & Debug
- Testing
- Operation & Maintenance



Polyinstantiation

- 2 or more rows have same primary keys but contain different data for use at different classification levels.
- Polyinstantiation is used as a defence against INFERENCE Attacks.

Noise & Perturbation Concept

Admin deliberately adds false / misleading data into DBMS to redirect or thwart INFORMATION CONFIDENTIALITY ATTACKS.

CH: 21 MALICIOUS CODE AND APPLICATION ATTACKS

Software Developer's worried layer

APPLICATION LAYER

PERSPECTIVE

THE ANTAGONISTS

- RECONNAISSANCE ATTACKS
  - IT probe, vul. + port scanning
- MALICIOUS CODE
- PASSWORD ATTACKS
  - Password guessing
  - Dictionary attack
  - Social engineering
  - Countermeasures
- APPLICATION ATTACKS
  - Buffer overflow
  - TOCTTOU
  - Back doors
  - Escalation of privilege and Rootkits
- MASQUERADING ATTACKS
  - session hijacking
  - IP spoofing
- WEB ATTACKS
  - SQL injection
  - XSS
  - XSRF

Where this malicious code come from?

Early days

- Skilled programmers put holes in s/w package or OS

Modern Days

1 Script kiddie

- Any person with minimal technical knowledge can download malicious code to launch attack against remote systems.

Amateurs

Plenty of free tools available to download for malicious code = ELEVATE CRIME

2 Organised crime

- Zeus Trojan Horse :- Eastern European organised crime seeking to infect systems with log keystrokes & harvest online Banking passwords

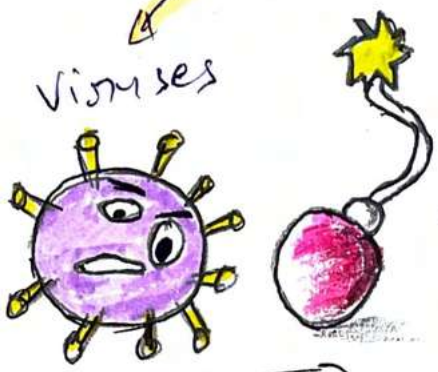
3 Advanced Persistent Threat (APT)

- Military units, intelligence agencies, shadow groups usually affiliated with governmental agencies

STUXNET

- APT Attacks are unique :- malware developer have access to zero-day exploits that are unknown to software vendors.

Malicious code

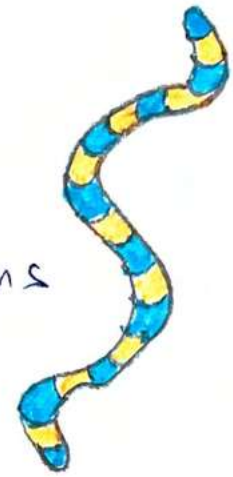


Viruses

Logic Bombs

Trojan Horse

Worms



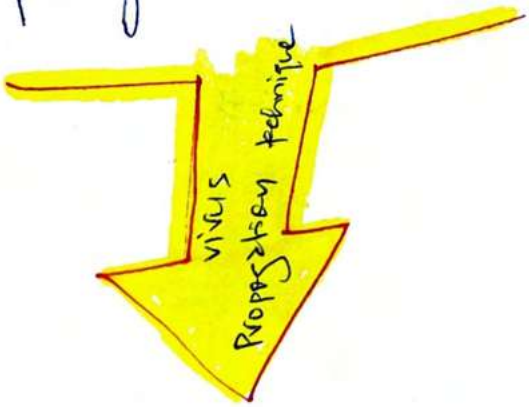
VIRUSES

Computer virus 2 main function

---- covid-19

(1) Propagation

- virus spread from one system to another system, infecting each machine



(2) Destruction

- Negatively impacts the confidentiality, integrity & availability of system Data

---- MBR vs BOOT SECTOR (CP. to x2)

<a> Master Boot Record (MBR)

CD/DVD

USB

----> OS Memory & Harddrive

- system reads infected MBR during boot process, loading entire virus into memory triggering delivery & virus payload

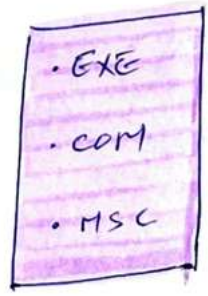
virus

<b> File Infector Viruses

F**** UP FILES

Virus

Attach



Files

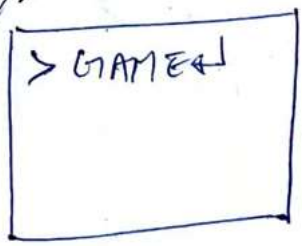
DO NOT DOUBLE CLICK

Variation : Companion virus

- They escape detection using file name similar to, but slightly different from legitimate OS file

game.exe → legitimate

game.com → virus



CMD

Execute virus so, avoid shortcut to execute files.

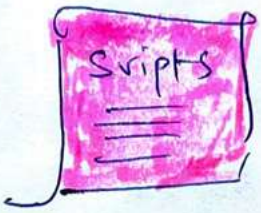
Boot Sector virus

Moves boot sector to another location on hard disk and then executes virus code instead of boot sector code. Most anti virus s/w scan for Boot sector virus.

<c> Macro Viruses

infects Microsoft office template

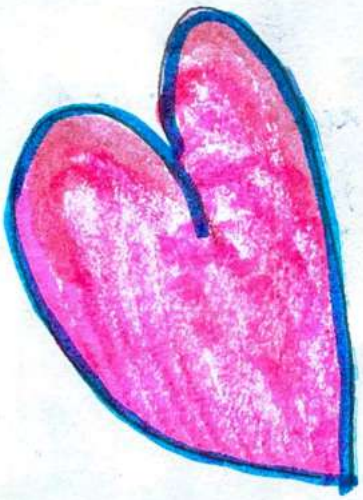
pick



⇒ To Automate Repetitive Task

mid 90's | 1999 | now

- macro virus started infecting documents
- Antivirus vendor had no defence as they never anticipated them.



1999

Melisa virus:
Use of word document that exploited security vulnerability in microsoft outlook to replicate

!
!
---. 2000

I love you virus followed on its heels

now

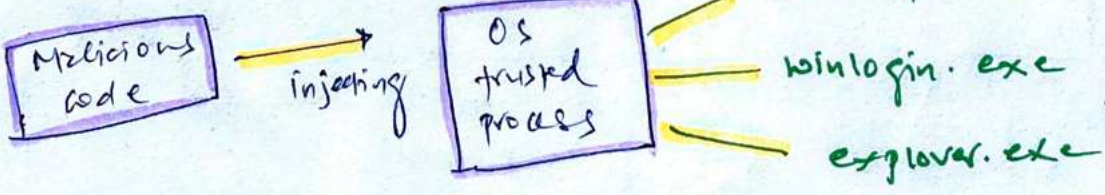
- s/w developers changed macro development environment,

Restricting the ability of untrusted macros to run without explicit user permission

↓

Drastic reduction of macro viruses.

<d> Service Injection Viruses



Even Antivirus running keep can't detect as viruses is inside the trusted process

→ Protect with latest security patches.

Boot Sector & Master Boot Record
(OSM Page 918)

ANTIVIRUS MECHANISMS

How Antivirus Package take action when VIRUS is FOUND?

Disinfect the affected files & restore machine to safe condition.

DISINFECT
+
QUARANTINE
+
DELETE

if doesn't know how to disinfect files, it will quarantine file so Admin can look up manually.

If policies / setting doesn't provide quarantine, antivirus package may delete the file to maintain system integrity.

Polymorphic viruses constantly change the signature & makes AV signature useless.

Antivirus Programs

Signature based detection

Annual s/s for updated definations / latest viruses

Analyze the behaviour of the software

Heuristic-based mechanism to detect potential malware infections

Suspicious file to quarantine & analyse with malware tool

↳ Blacklisting

↳ whitelisting

Modern AV products = More than virus

- rootkits
- Trojan Horse
- worms
- Logic Bombs
- spyware
- Email + web protection

Tripwire Data Integrity Assurance program

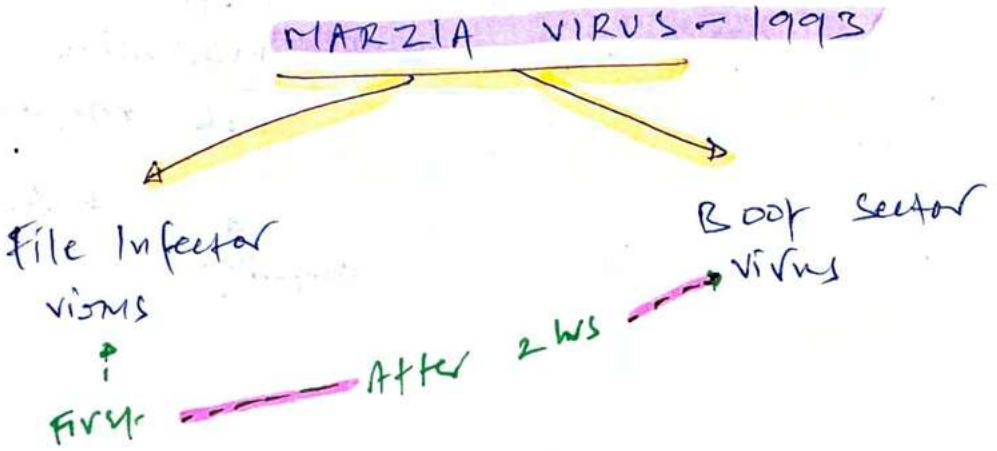
- Secondary antivirus functionality
- Alerts admins for unauthorised file modifications

VIRUS TECHNOLOGIES

4 specific types of viruses that use sneaky techniques to escape detection

1. Multipartite viruses

- Use more than one propagation technique



2. Stealth viruses

- Hide themselves, tamper with OS to fool AV thinking everything is functioning normally.

OCEAN 11 - 911 lines diverted

- Stealth virus stays hidden by monitoring service calls.

E.g. writes malicious code to boot sector & then modifies file access functionality to cover the tracks.

AV created the code but it takes longer to detect.

(3) Polymorphic Viruses

Covid-19 → Delta → Omicron → ?.

- Modifies its own code as they travel from system to system.
- Virus's propagation & destruction technique remains same but signature of the virus differs everytime it affects the new system.

(4) Encrypted viruses

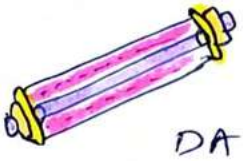
New cryptographic key = New infection

- Use cryptographic techniques to avoid detection

* Outward appearance similar to polymorphic (use different signature for new infection) But, it doesn't change code to modify signature, instead it alters the way they store signature on the disk.

LOGIC BOMBS

Indiana Jones - once treasure is found - Everything fails (crushes gold)



DA VINCI CODE → If water breaks = Destroy the map

Malicious code that lies dormant until it triggers a specific occurance

- Time
- Program launch
- website login

Viruses + Trojan Horse → contains logic bomb components.

Michael Angelo Virus (1991) — 6th march

North Korea → South Korea

TROJAN HORSES

Behind the scene malicious payload

TROY. - watch the film.

Xbox Trojan Horse

→ Not to play the game but to generate advertising revenue from web page.

Recent Category of Trojan

Rogue Antivirus software

Tricks user to install Antivirus package, once run

→ steals personal data

→ Ask for payment = Post payment, it disables trojan!

Ransomware

Cryptolocker Attack

- Utilized trojan horse on windows.

Encrypt Files

Pay Bitcoin

→ Decrypt

→ OR Private key will be deleted

Worms

- Threat to modern Internet
- significant risk to network security
- As dangerous as malicious code but with added twist
  - worm propagates itself without human interventions

Twist from virus/ malicious code

Code Red worm

- 2001: attack on running unpatched web server on Microsoft Internet Information Server (IIS)
  - 3 malicious actions.
    a) Normal webpage into
    Hacked by chinese worm. com
    b) Attack on random IP Address.
    if host = IIS + unpatched?
    → compromised system
    c) DDOS Attack on White House
    IP = 198.137.240.91

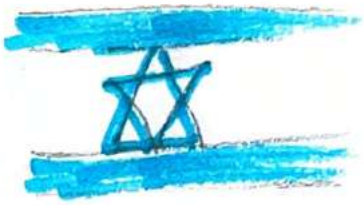
Stuxnet

- 2010: used various propagation techniques
  a) Unprotected administrative shares on local n/w
  b) Exploit zero-day vulnerabilities on window server service & windows print spooler service
  c) Corrupt system using default database password
  d) Spreading via infected USB drives.

SIEMENS SYSTEM → NUCLEAR WEAPONS

Sol: Patch Management (24x7x365)

Stuxnet



story

Virus was designed as American-Israeli project to sabotage Iranian Nuclear weapon program

2 Evolutions in the world of malicious code

Worms can cause physical damage to facility

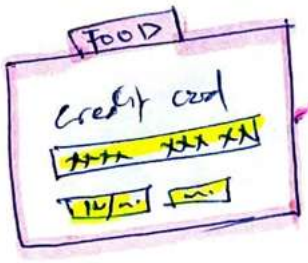
Use of malicious code in warfare b/w nations.

End of viruses, logic bombs, worms, trojan

BUT, 2 other types of software interfere

SPYWARE

- Monitors actions & transmits important details to remote system

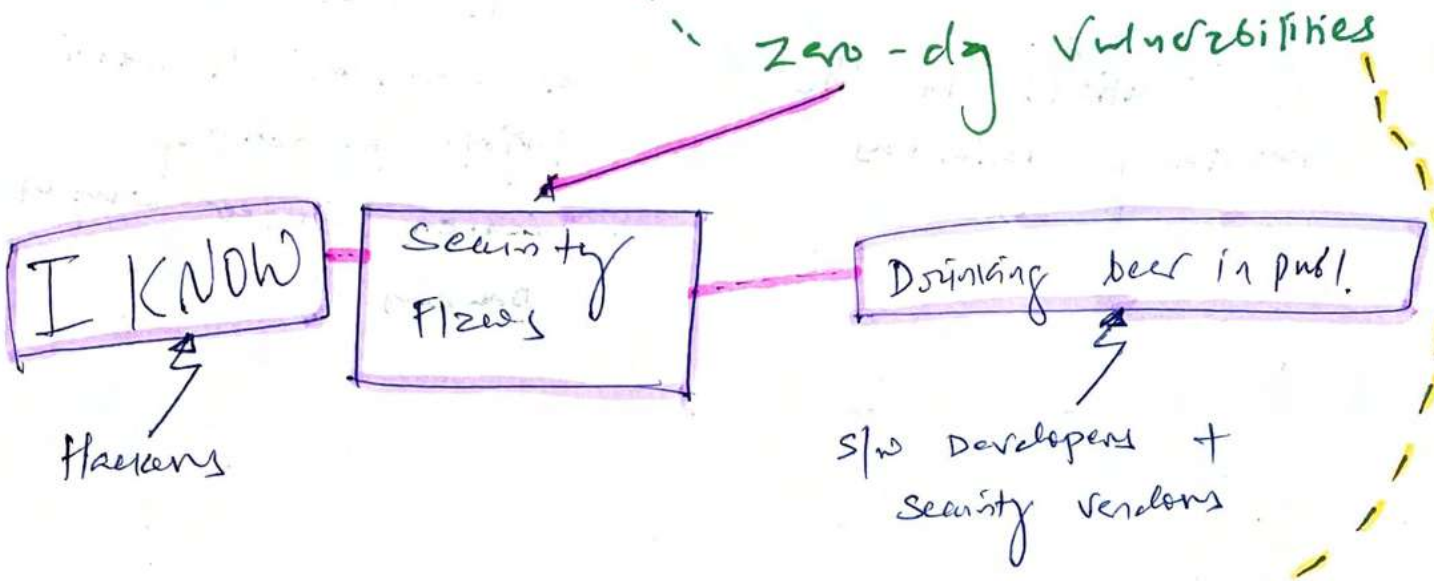


Transmit to fraudster to resell to black market

ADWARE

- Display Ads on infected computers

Zero-Day Attacks



2 Reasons why it happens.

A) Window of Vulnerability :- Delay b/w discovery of malicious code to issue of new patch

B) Lethargic Administrator :- Slow update on system.

Sol. → Strong patch mgmt + configuration mgt policy & standards

→ Defence-in-depth controls — Don't just rely on one controls

Multiple Boyfriends.

PASSWORD ATTACKS

- Password Guessing
- Dictionary Attacks
  - Tool: John The Ripper
  - New Variant: Rainbow Table Attack where Attacker simply search for Hash value in rainbow table to determine user password.
- Social Engineering
  - What's your password?
  - I am from IT support
- Phishing Attacks
  - Spear phishing — Use personal information to design attack more authentic.
  - Whaling Attacks — To target senior executives (High-valued targets) — CFO
  - Vishing Attacks — over phone — ATO

USE SALT

SAFEGUARD
- long password + special characters
- MFA
- Password safe

APPLICATION ATTACKS

Buffer Overflows vulnerabilities

- Happens when developer don't take input validation seriously.
- It can crash the system or even allows users to execute shell commands & gain access to the system. (allows to run arbitrary commands)
- Allows attacker to modify content of system/memory.

TOCTTOU

- Time of check to time of use
- If Admin revoke specific Permission to user but verification never applies till user login for next time. For this, user can simply login (never log-off) so new verification will never apply & he/she will have access to resource indefinitely.

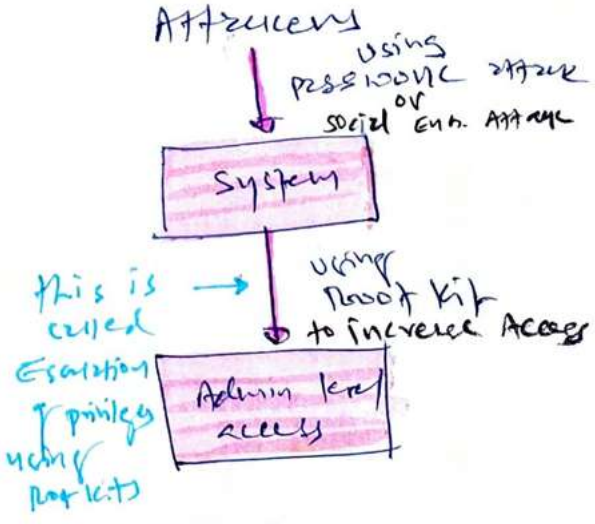
Back Doors

(1) Irresponsible Developers who wants to bypass authorization during development/debugging left this in production too.

(2) Malicious code can create back doors.

Escalation of Privilege and rootkits

- We can launch Escalation of privilege attacks using rootkits.



- Soln: Patch that down system.

WEB APPLICATION SECURITY

XSS : cross-site scripting

- occurs when Web Applications contain some kind of reflected input.

Dave <SCRIPT> alert ('hello') </SCRIPT>

This is input = Web Browser process input + execute malicious code script

- Key to this attack = it's possible to embed form input in a link.

- Sol.

(a) Perform input validation

(b) Never allow <SCRIPT> try in a reflected input field.

XSS attacks exploit the trust that a user has in a website (browser) to execute code on user's computer.

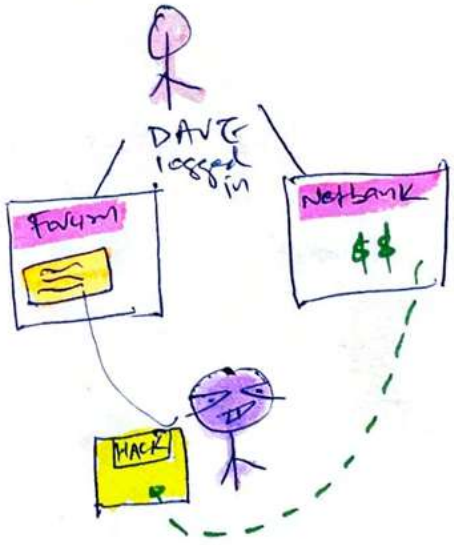
SQL Injection

P.T.O

XSRF : Cross-site Request Forgery

XSRF attacks exploit the trust that remote sites have in user's system to execute command on the user's behalf.

- XSRF attacks works by making reasonable assumptions that users are often logged into different website at same time



Sol:- Create Web App that use secure tokens

- Only accept URL request that originated from their site.

OPPOSITE

SQL INJECTION

- Unexpected input to Web Application
- It doesn't use input to fool user. Instead, SQL injection attack use unexpected input to gain unauthorised access to an underlying database.

--- Dangerous than XSS

- Expected input to Web Application

WEBSITE
- then: STATIC
- now: DYNAMIC

Birth to

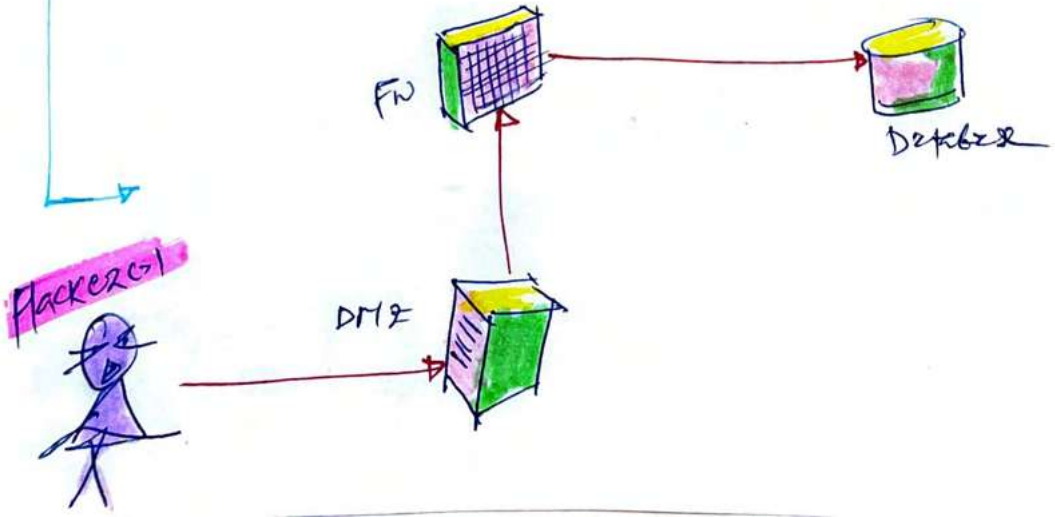
DYNAMIC WEB APPLICATIONS

Birth to

DATABASES
- Create content on demand based on user request.

THE CONTEXT

→ Created complexity as path does exist from Internet to Internal via DMZ



Flaw in Web Application [DMZ] → High chance of Database tempering [INTERNAL]

* SQL Injection Attack

- Web Application use SQL query to obtain information from Database.

BUT, if Web application doesn't perform proper INPUT VALIDATION, user can insert their OWN SQL CODE to influence Web server.

NOW : SELECT * FROM transactions where ac_number = 46 ; DELETE * FROM transactions WHERE 'a' = 'a'

first statement retrieves all the records for account number 46, then

Second statement, deletes all the records from Database!

WHOOOOPS!

* Protection against SQL Injection

1 Use Prepared statements

Like Ready made clothes.

- Prepared statements limits application's ability to execute arbitrary code
- Prepared parameterized query stored in SQL database that only Database admins / developer can modify with appropriate access.
- Web Applications calling Prepared statements may pass parameters to it but it may not alter the underlying structure of SQL statement.

2 Perform Input validation

- Limits types of data a user provides in a form.
- Removing character(' ') could prevent attack
- Whitelist validation: code verifies that user-supplied input matches the expected pattern before submitting to database

3 Limit Account Privileges

- least privilege
- Access based on business need to know.

Reconnzissance Attacks

First phase of Pen Testing

No trick like malicious code → Direct Attack on weak points

Developer use automated tools

1 IT Probes
- nmap
- ping sweep

- Ping attempt to entire network
- Disable ping for external network and on firewall, block ICMP

2 Port scans

Attacker → Port scan software → Port 80 : open → EXPLOIT.

3 Vulnerability scans

Intruder → scans Entire Network → To Find Vulnerability → Exploit

Patch bzbg! Patch it.

Patch Me Baby One more time ~~~

Masquerading Attacks.

Below 18 ?

No → Buy Alchohol. No problem

YES → Borrow Driviling License of 18 + → Buy Alchohol. No problem

- Easiest way to gain a system access is to impersonate someone who does have appropriate permissions.

2 most common masquerading attacks.

IP Spoofing

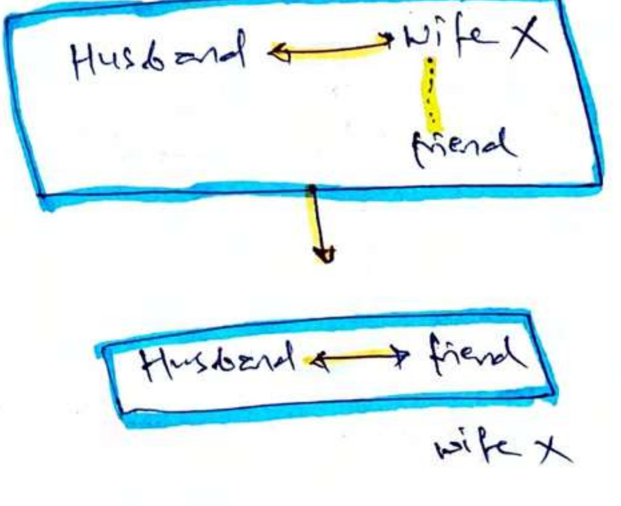
- malicious user reconfigure IP of trusted system (18+ DL)

↓

Attempts to gain access to external resources.

Session Hijacking

- malicious user takes over identity of authorised user.



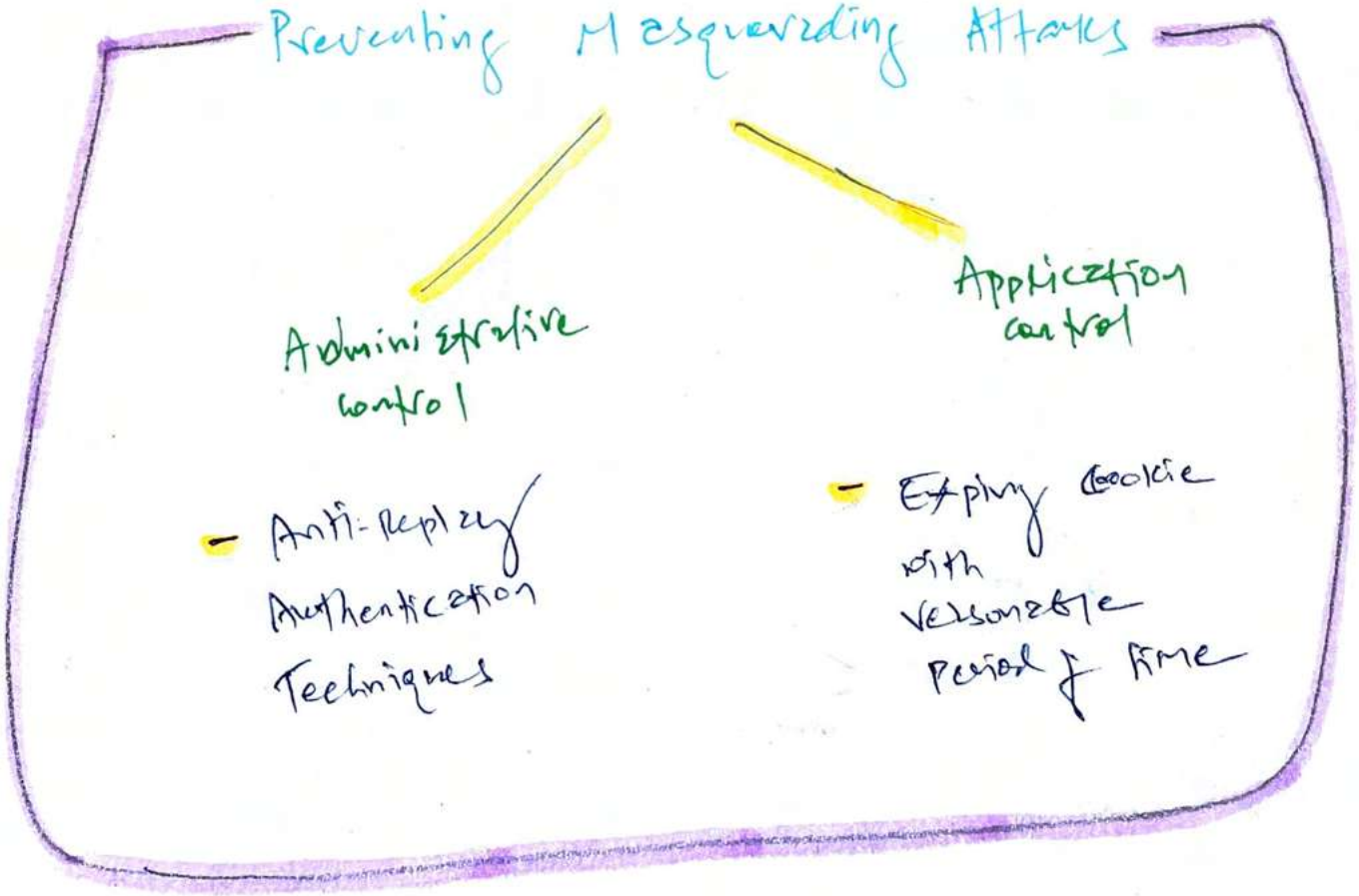
P.T.O

3 Filtering Rules to eliminate majority of IP Spoofing Attacks.

<a> Packets with internal IP don't enter the network from outside.

<b> Packets with External source IP don't exit network from inside.

<c> Packets with private IP Address don't pass through router in any direction.



Buffer overflow → Input validation

TOCTTOU

Backdoors

Escalation of privileges & Rootkits → patch.

XSS → Input validation, NO </SCRIPT> tag

XSRF → Use Secure Token, Accept original URL from site

SQL injection → Input validation, Limit Account privileges, Use prepared statements

Masquerading Attack (IP spoofing + Session Hijack)

- Remember those 3 filtering rules (A.P.O)
- Anti-replay Authentication
- Expire cookie time

Dictionary Attack → John the Ripper

→ Rainbow Table → Use salt (variant)

Password Guessing → long phrase + special characters

Social Engineering → phishing

↓ variant

Dumpster Diving → Shred paper, wipe electronic media.

ZERO-DAY ATTACKS

→ patch & config. mgmt policy

→ Defense-in-depth