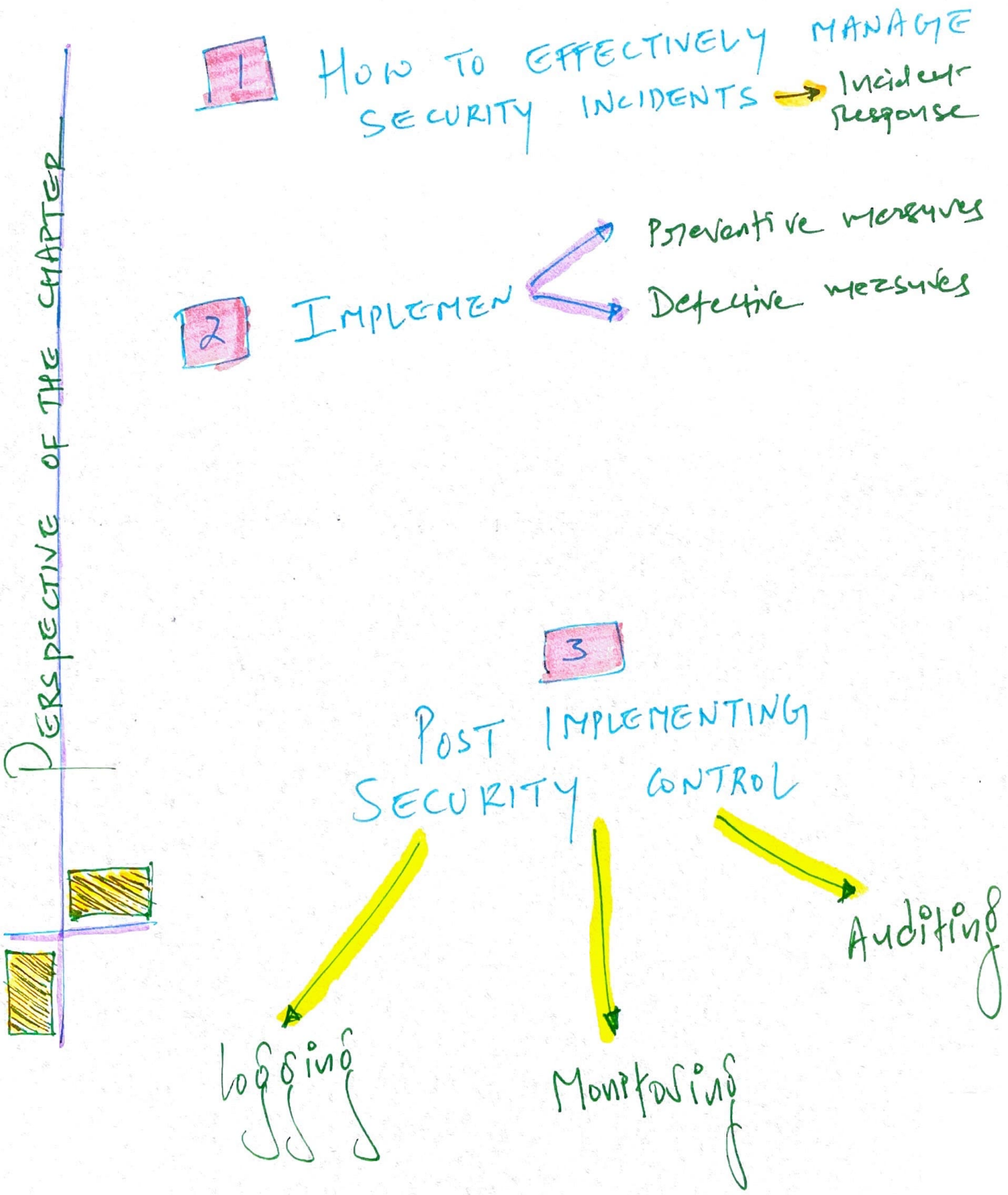
17. Preventing and Responding To Incidents



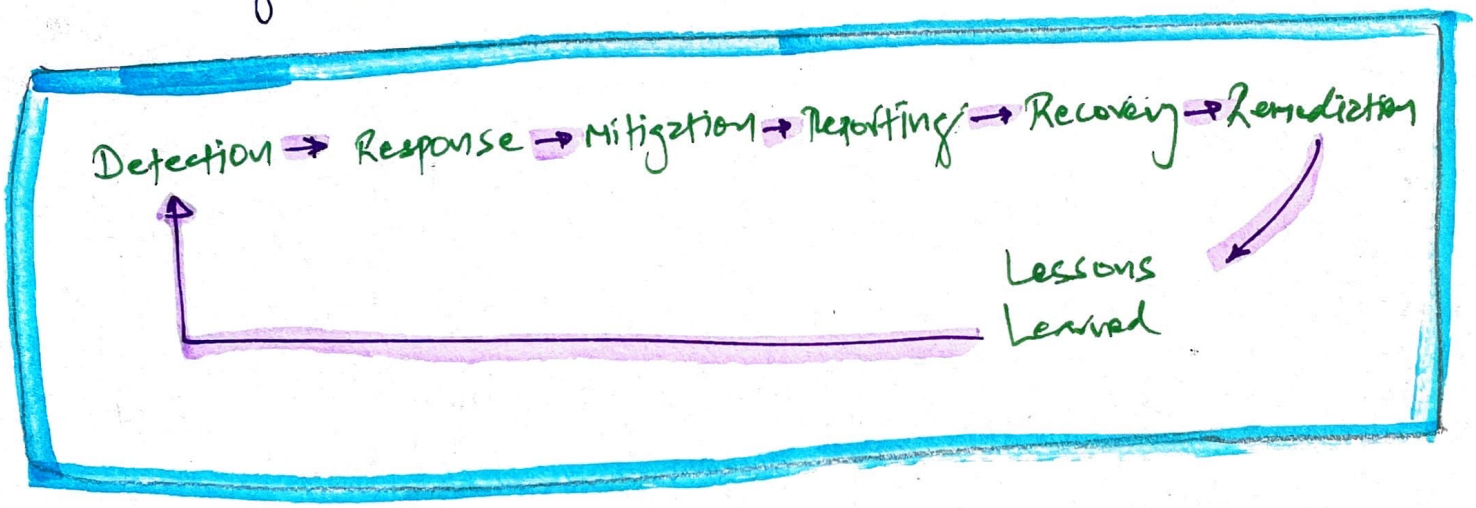
1 MANAGING INCIDENT RESPONSE

REVISIT
P.T.O
END

Incident mgmt
Primary Goal
- Minimize the impact of the organization

Incident Response Steps

Any event that affect CIA of organization's assets.



Few Important Points

↳ Incident response doesn't include counterattack as well 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

↑

configuration mgmt + change mgmt policy will help

→ Check ACL

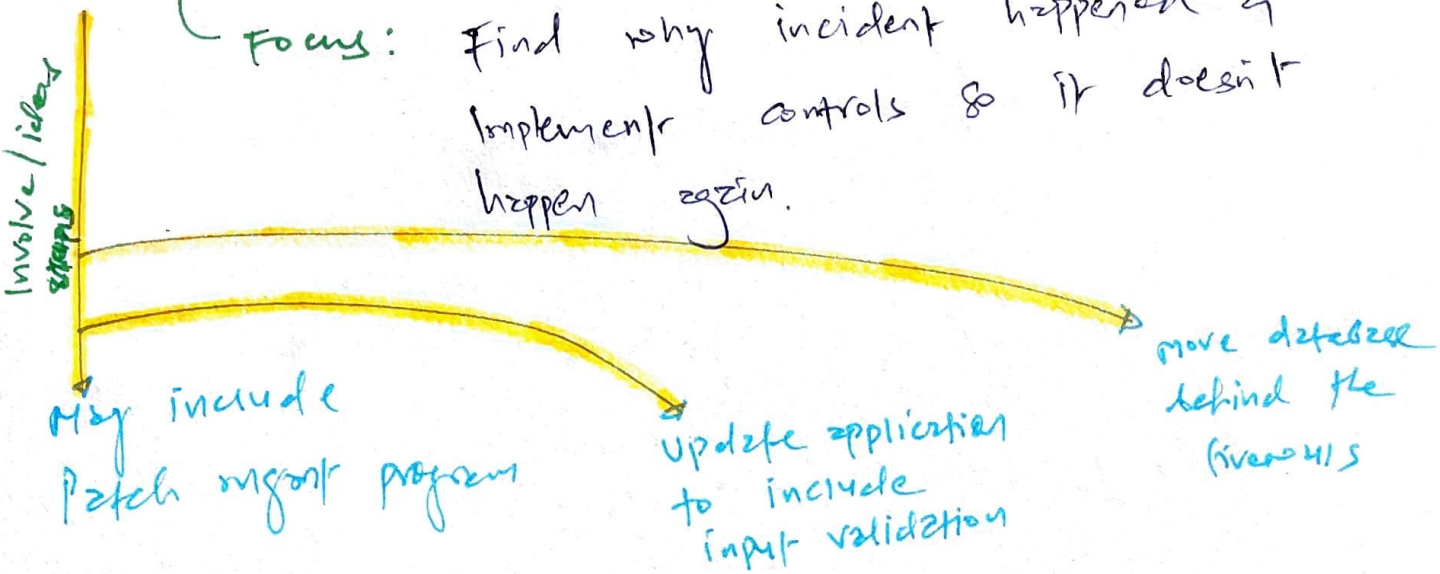
→ IAM

→ Disable unnecessary services / protocols

→ Install patches

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

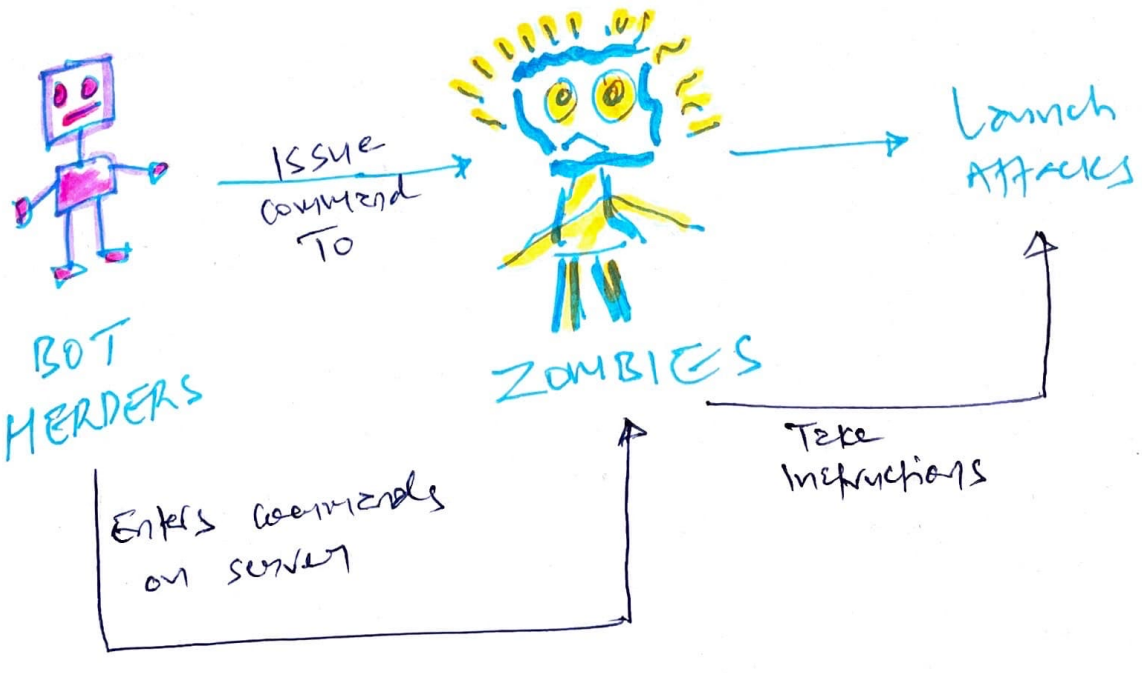
chapter Focus: Preventive security controls against well-known attacks

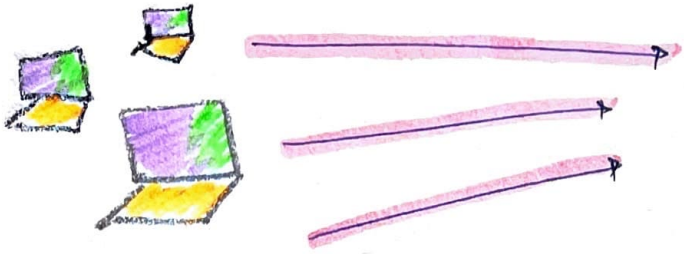
Basic Preventive measures → disable unneeded service + protocol

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

* Understanding Attacks

1 BOTNETS — Robots





Affected PCs with malicious code

Joints

BOTNET

Botnet preventions

Defense-of-depth (multiple controls)

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

up-to date Browsers & plugins

Educate + Training users.

DO NOT CLICK.

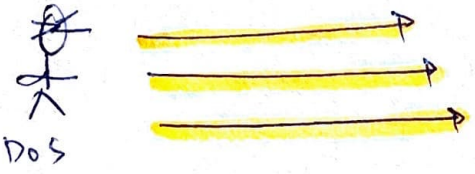
cyber sketch :- Botnets for IoT

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

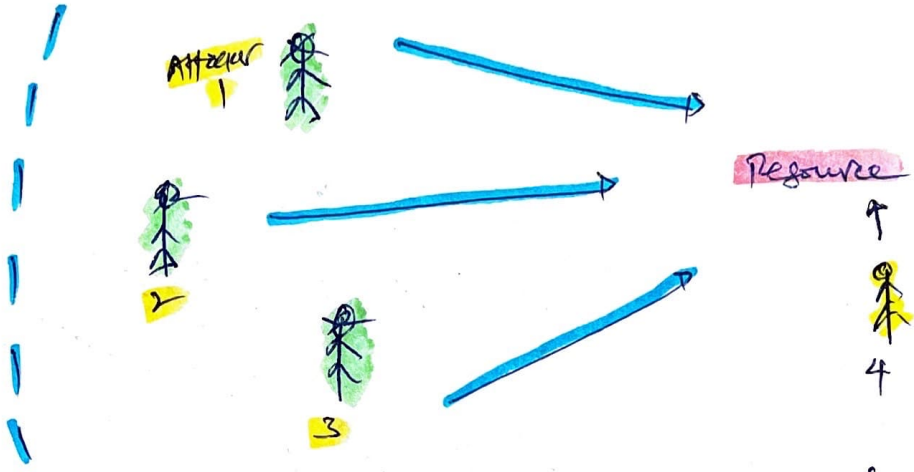
(2) DENIAL-OF-SERVICE ATTACKS (DoS)

Overwhelm resources

Exploit known vulnerabilities

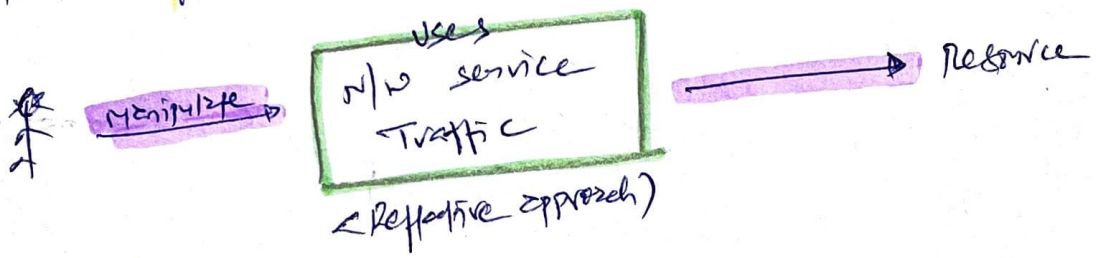


Distributed DoS (DDoS)



Attackers use BOTNETS to launch DDoS Attack.

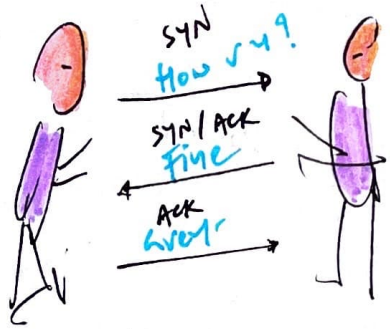
Distributed Reflective DoS (DRDoS)

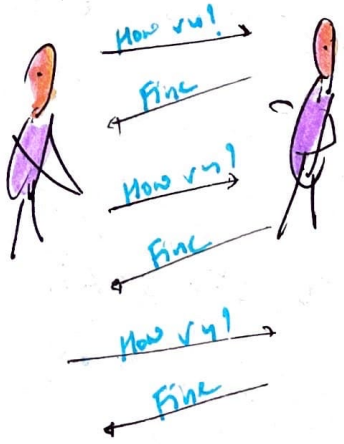


- DNS poisoning
- Smurf Attack

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.

↓

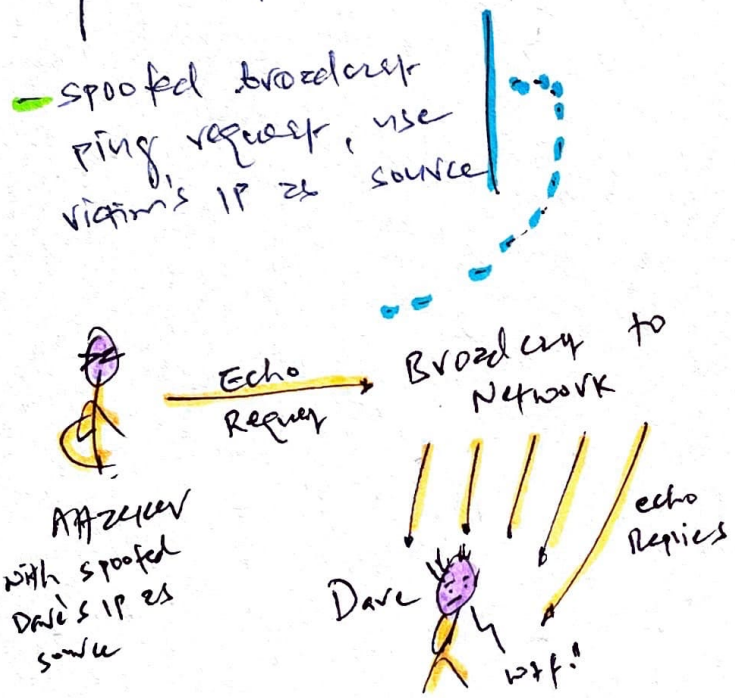
Session cookies

- Small reloads consume very few system resource

(4) SMURF & FRAGGLE ATTACKS = DoS Attacks

Flood Attack = uses ICMP instead of TCP SYN packets

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



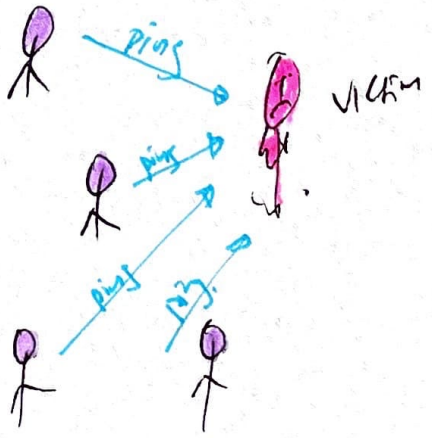
Prevention

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

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

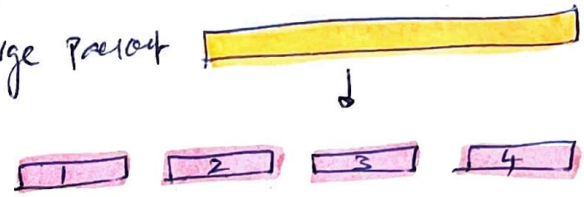
System crash

Buffer overflow

Sol:- patch

7 TEARDROP

Large packet



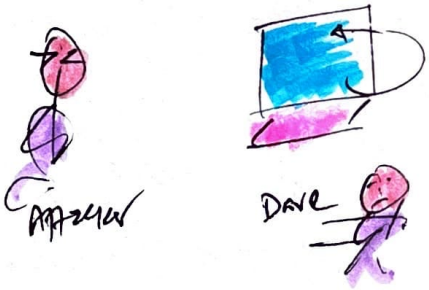
Attack

Coil. put the data back to normal

Sol!
+ IDS

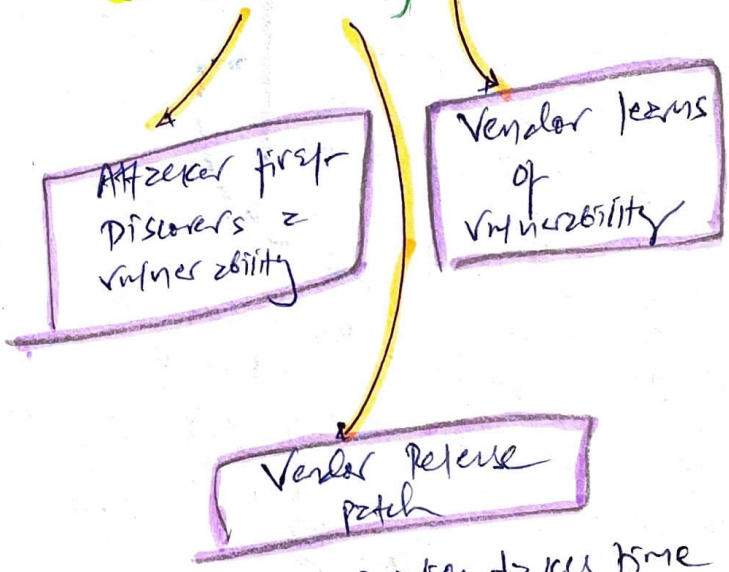
8 LAND ATTACKS

- 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



- organization takes time to apply patch

Microsoft → PATCH TUESDAY

Have patch mgmt policy → 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.

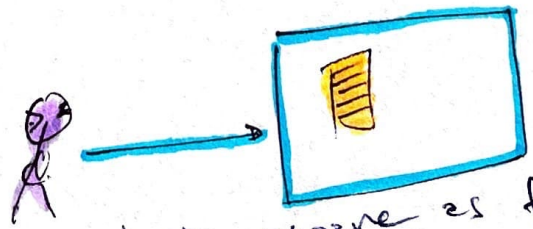
Takes advantage of unpatched systems.

- Malvertising Ads

FREE TOOL MICROSOFT

uses

- 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 (WHM)

- copying traffic b/w two parties

Store-and-forward (Proxy mechanism)

- client & server think they are directly connected but attacker captures & forward 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$ traces benefit of 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)

Nexp → 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.

Logs → IDS

Sensor on Router / Firewall

Evaluates data & detect malicious behavior using 2 methods

Knowledge-Based Detection

can detect known attacks.

- signature based detection

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.

False Alarms

Accurate Alarms

SOC

challenge

+

Resource Productivity

SIEM

Splunk / StreamDriven

Collect real-time data from multiple ~~data~~ 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

Go HIDS

Want granular

Disadvantage

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 speech

DAVE

Secure HTTPS

IPDS

Malicious Site

SOLUTION

can't detect malicious code] ...decrypt → IPDS

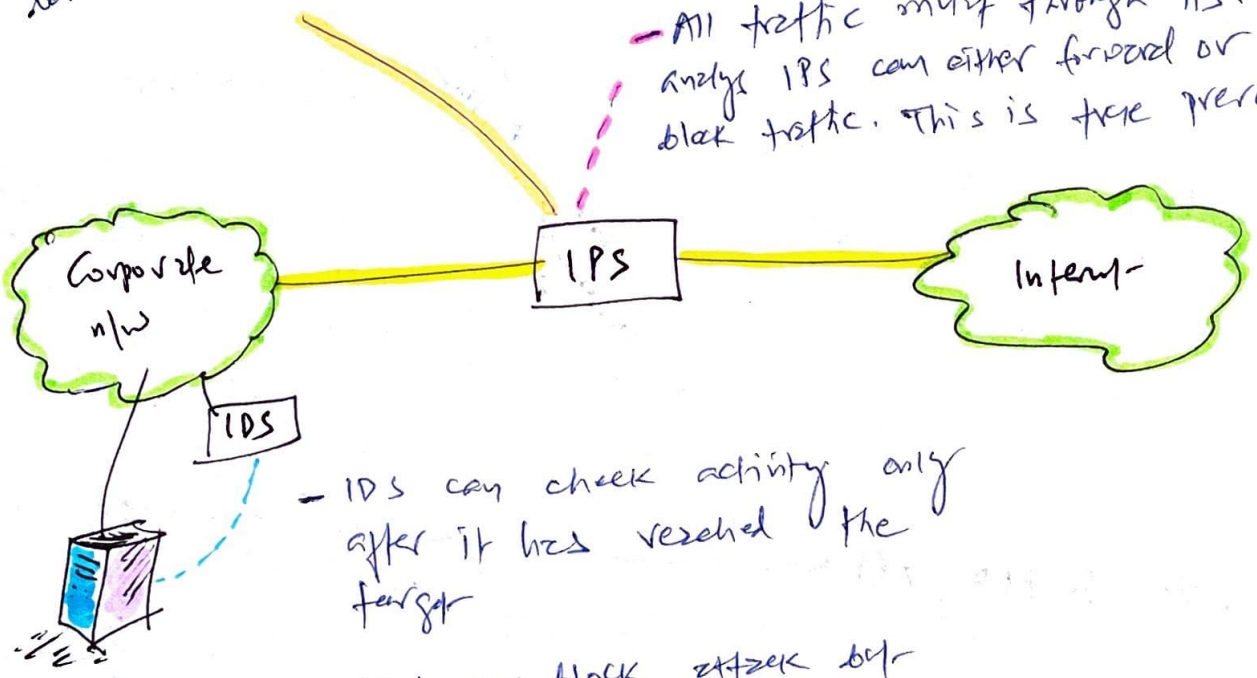
USE OF TLS DECRYPTORS

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 → / hour

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

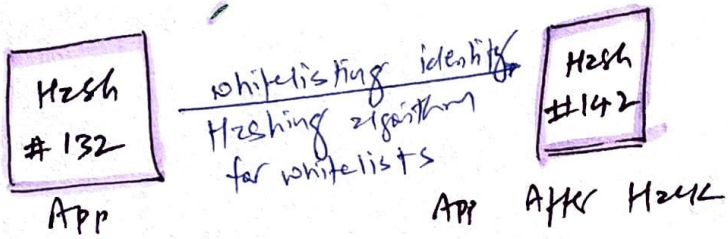
Whitelisting & Blacklisting = Goal: to prevent users running unauthorised Apps / prevent malware infections

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 antimalware 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

↑

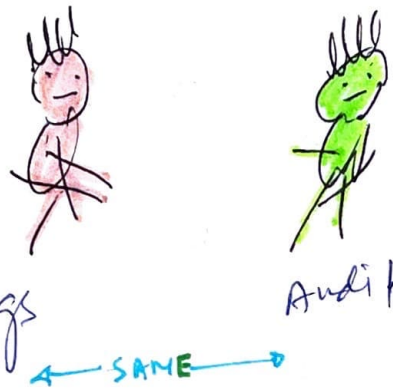
Hacker (Good one)

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



Common log types

- Security Logs
- System Logs
- Application Logs
- Logs from privileged Accounts
- Firewall Logs
  - traffic to/from firewall
- Proxy logs
  - which site user access
- Change logs
  - Input for DR + alignment process

Note - Don't forget to record event / logs from Privilege / root accounts. This prevents attack from malicious insider

CyberArk

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

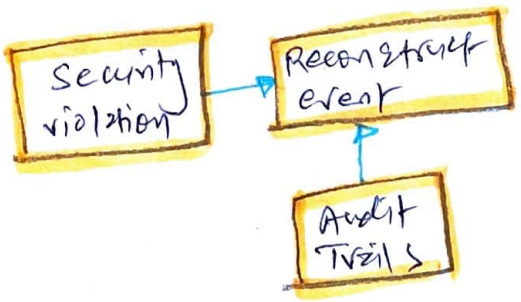
- Reconstruct activity - forward or reverse order to find culprit - or why exactly happened.
- As evidence for prosecuting criminals

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

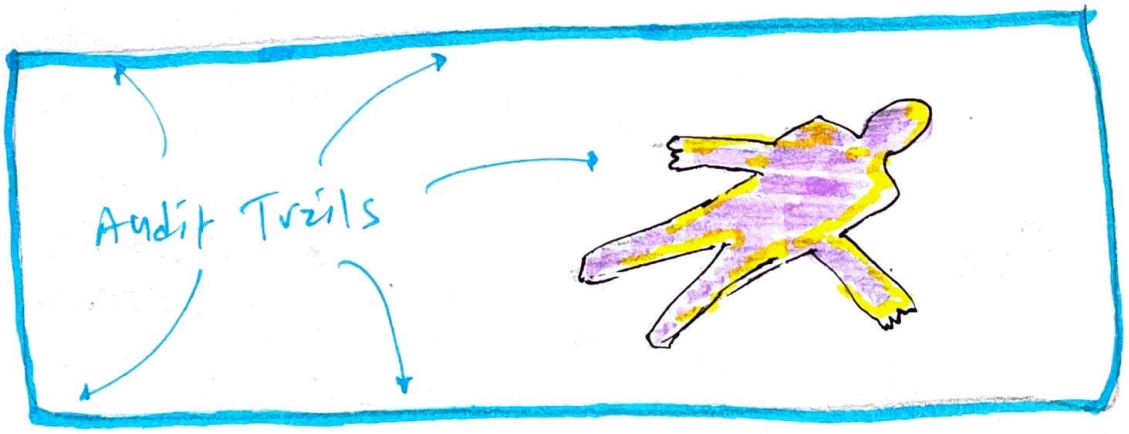
After NTP, NIST servers responds with encrypted & authenticated time messages.

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.

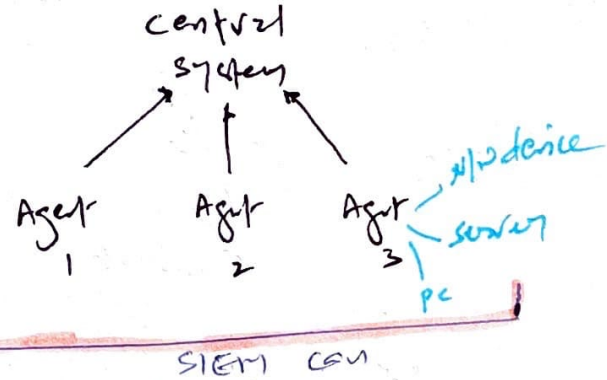
SAMPLING (Data Extraction)

$$$$

data Reduction

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

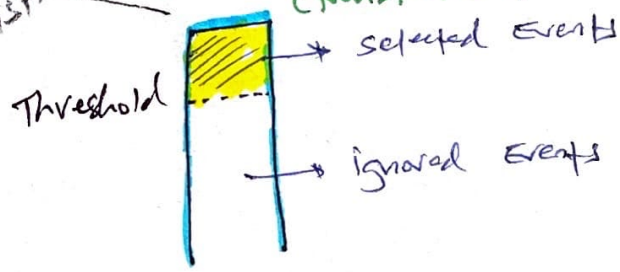
SIEM (Security Information & Event Management)



- 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

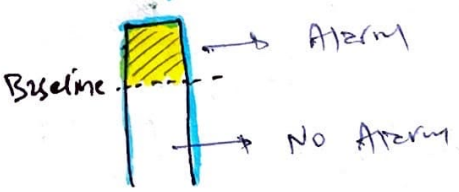
CLIPPING LEVELS (Noniztism)

NON Statistical $$



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.