Date _____ Day _____

CHAPTER #08

→ TYPES OF INTRUDERS – Based on Motivation

① Cyber Criminals – Motivated by Money
- ↳ Activities include
  - ↳ Stealing identities
  - ↳ Stealing bank info
  - ↳ Corporate Spying
  - ↳ Stealing or locking data (ransomware)
- ↳ Often work in groups
- ↳ They buy/sell → stolen data, hacking tools

② Activist / Hacktivists – Motivated by Political / Social Cause
- ↳ Attack to support a cause or protest something
- ↳ Activities include
  - ↳ website deface (unauth access to website changing their content, images, code etc)
  - ↳ leak data

③ State Sponsored Hackers
- ↳ Supported by countries for espionage / sabotage
- ↳ Called Advanced Persistent Threats (APTs) bez:
  - ↳ they are skilled
  - ↳ work secretly
  - ↳ Stay inside network for months/years

Date _____ Day

④ Others
↳ Classic hackers doing it for fun / reputation
↳ Includes:
↳ Those discovering new security vulnerabilities
↳ Hobbyists using freely avlbl hacking tools
↳

→ SKILL LEVELS OF INTRUDERS

① Apprentice (Low)
↳ Use ready-made hacking tools
↳ Cannot create their own attacks
↳ Most common type of attackers
↳ Easiest to defend against

② Journeyman (Medium)
↳ Can modify existing tools
↳ Can exploit new or similar vulnerabilities
↳ Harder to defend against
↳ Found across all categories

③ Master
↳ Can discover new type of vulnerabilities
↳ Can create powerful original attack tools
↳ Work often for → state sponsored groups
↳ high profile underground

Date _____ Day _____

→ Examples Of Intrusion
- → Remote Root compromise of an email server
- → webserver defacement
- → guessing cracking pswds
- → Copying databases containing credit card numbers
- → Viewing sensitive data without authorization
- → Running a packet sniffer
- → Distributing pirated software
- → Using an unsecured modem to access internal network
- → Impersonating an executive to get information
- → using an unattended workstation.

→ INTRUDER BEHAVIOUR

① Target acquisition & information gathering
- ↳ Attacker studies the target
- ↳ They collect info like
  - ↳ what sys the target uses
  - ↳ Public details about the orgs
  - ↳ social media info
  - ↳ what software/server are running
  - ↳ IP Addr, open ports & network structure

② Initial Access
- ↳ The attacker gets the first entry into the sys.
- ↳ Exploiting a remote vulnerability

Page No

Date _____ Day

↳ guessing weak psuds
↳ pishing attack
↳ installing malware via social engineering

③ Privilege Escalation

↳ Once inside, attacker try to incr their access lev
↳ Eg:
  ↳ Taking adv of local vulnerabilities
  ↳ abusing misconfigurations
  ↳ Using stolen admin Ep suds

④ Info Gathering or System Exploit

↳ Now the attacker uses their access to:
  - steal sensitive data
  - modify or delete information
  - Spy on the sys

↳ Achieve the purpose of attack

⑤ Maintaining Access

↳ Attackers don't want to loose access once gain
↳ So they install tools that let them come back anytime, such as
  - backdoors
  - hidden malware
  - secret user account

↳ Stay inside for long term.

Date Day

Covering Attacks

↳ To avoid getting caught, attackers try to hide all evidence

↳ They do:
- delete or alter logs
- install rootkits to hide files / processes
- erase malware traces

• INTRUSION DETECTION (IDS)

→ Security intrusion — unauthorized act of bypassing the security mechanisms of a system.

→ Intrusion detection — A hardware or software function that gathers and analyzes information from various areas with a computer or a network to identify possible security intrusions.

→ Components of IDS

① Sensor -

↳ Collects raw data from the system

↳ They watch
- ↳ Network Traffic
- ↳ Log files (sys logs, server logs)
- ↳ system calls (what programs are doing)

Date _____ Day

↳ Just observe and send data to the analyzer

↳

(2) Analyzers

↳ Analyst study the data received from sensors

↳ They decide

↳ Is this normal behvior?

↳ Or is this an attack?

↳ If they detect something suspicous, they produce an alert.

↳ They may also:

↳ Show evidence of the attack

↳ Suggest what actions to take

↳ Store data for future investigation

(3) User Interface

↳ This is what the admin sees.

↳ Through the interface, the user can:

- view alerts
- view logs
- manage the IDS

Date _____ Day _____

→ Types Of IDS

① Host-Based IDS (HIDS)

↳ It monitors a single computer/server
↳ It watches:
  ↳ system calls
  ↳ running processes
  ↳ file changes
  ↳ logs on that host
↳ Detects attacks happening inside a specific machine

② Network-Based IDS (NIDS)

↳ It monitors network traffic accross a network segment or device
↳ It inspects:
  • packets • protocols • network connections
↳ Detect attacks travelling through the network

③ Distributed / Hybrid IDS

↳ It monitors data from multiple sensors, both host-based & network-based
↳ It collects:
  • HIDS data from servers
  • NIDS " " network devices
  • Sensor data from firewalls, router, switches

Date _____ Day _____

↳ Provides a full picture of attacks happening acr the entire organization.

Network-based IDS	Host-Based IDS
(1) Broad in scope	(1) Narrow in scope, monitor specific activities
(2) Examines pkt header & entire packet	(2) Donot see pkt headers
(3) Near real time response	(3) Responds after a suspicous entry
(4) Host independent	(4) Host dependent
(5) Bandwidth dependent	(5) Bandwidth indep.
(6) No overload	(6) Overload
(7) Detects network attacks, as payload is analyzed	(7) Detects local attacks before they hit the network
(8) High false +ve rate	(8) Low false +ve rate
(9) Better for detecting attacks from outside	(9) Better for detecting attacks from inside

Date _____ Day _____

→ Basic Principle Of Intrusion Detection

↳ Security sys like authentication, access control and firewalls try to stop attacks, whereas, IDS → tries to detect attacks that slip through.

↳ Importance of IDS → intruders

(1) Easly detection reduces damage
- ↳ kick them out before any damage
- ↳ or at least limit the damage
- ↳ Recover fast

(2) IDS discouroges attack
- ↳ If attackers know your sys has strong IDS, they may not even try to attack

(3) Helps improve security systems.
- ↳ IDS logs attack
- ↳ helps security teams understand
  - how attackers try to break in
  - what weakness they target
- ↳ helps improve future security

Date _____ Day

→ Main idea behind IDS

Attackers behave differently than normal users

↳ So IDS tries to identify these differences

But,

↳ Normal users may sometimes behave strangely

↳ Attackers may try to behave normally

Due to this the ~~false~~ "false positive" (IDS classifies a normal user as attacker) is increased

Eg: 9 forgot password & tries to login multiple times.

But if we try to limit the false positive rate, then "false negative" (attacker classified as normal user) is increased. or

Eg: Attacker uses valid credtials → seems normal

↳ So the IDS design must be balanced.

- **Outsider Attack**

↳ Easier to detect

↳ Their behviour is clearly diff from normal users

Inside Attack

↳ Hard to detect ↳ They are legit user misusing access

Day

Date

↳ Their activity often looks normal
↳ Only small diff from normal behaviour.

→ **Base-Rate Fallacy**

↳ Even if your IDS is very good, it will still generate many false alarms because real attacks are extremly rare compared to normal behaviour

↳ Eg:
Suppose our ID is:
- 99% accurate for true attacks (detection rate)
- 1% false alarm

Now for 1,000,000 daily events on our server
↳ Actual attacks → 10

So now,
10 actual intusion x 99% = 9.9 ≈ 10 detected
↳ TRUE ATTACKS
1% false alarm rate x 999,990 normal events
↳ = 9,999 false alarms

Therefore we get only
10 real alarms & 9,999 false alarms

↳ So admin stops taking IDS seriously, this is base-rate fallacy

Date _____ Day _____

→ Requirements Of An IDS

1. Run continually with minimal human supervision
2. Recovers from crashes
3. Protect itself from being modified or bypassed
4. Use low system resources
5. Match the organization's security policy
6. Adapt to changing user/sys behaviour over time
7. Scale to monitor many hosts
8. Continue working even if some parts failed

• ANALYSIS APPROACHES

- Anomaly Detection —
  - ↳ Collects data on normal behavior of legitimate users over time
  - ↳ Compares current behaviour to this baseline
  - ↳ Flags behaviour that deviates significantly

- Signature / Heuristic Detection —
  - ↳ Uses known malicious patterns (signatures) or attack rules (heuristic)
  - ↳ Compares current activity to these patterns
  - ↳ Also called misuse detection
  - ↳ Can only detect attacks it already knows

Date _____ Day _____

① Anomaly Detection

↳ First builds a model of legitimate user behaviour during a training phase

↳ This model is then used in the detection phase to compare current behaviour & classify it as normal or anomalous.

↳ Training may occur at fixed times or accordingly

↳ Classification Approaches:

(1) Statistical ↗ like averages & trends over time

↳ Use univariate, multivariate or time series statistical models to analyze behaviour

(2) Knowledge-based

↳ Uses expert-defined rules that describe legitimate behavior

(3) Machine Learning

↳ Automatically learns classification models from training data using data-mining methods.

↳ Key Limitation

(1) IDS Anomaly detection models are usually trained only with legitimate data

(2) Lack of anomalous data ~~rede~~ reduces the effectiveness, especially of machine learning approaches, ~~since unknown attacks must still be~~

Date _____ Day _____

(2) Signature or Heuristic Detection

↳ they sys watches events happening in the computer or network

↳ It checks these events using:

- Signatures → known patterns of malicious activity
- Heuristic rules → rules that describe suspicious behaviour

(1) Signature-Based Detection

↳ Compares current data with a large list of known malware patterns

↳ Commonly used for

- Antivirus software
- Network Scanners
- NIDS (Network IDS)

↳ Advantages

① Fast & efficent

② Uses fewer resources

③ Widely trusted & used

↳ Disadvantages

① Requires constant updates to add new signatures

② Cannot detect zero day attacks (unknown new attacks)

Date _____ Day _____

② Rule-Based Heuristic Detection

↳ Uses rules to detect

↳
- Known attacks
- Attacks that use know weakness
- Suspicious behaviour that still looks normal

↳ Rules are usually specific to the OS or machine

↳ Rules are built by

↳ Studying attack tool found online

↳ Getting input from sys admin & security expert.

Eg: SNORT is popular rule based NIDS that uses many predefined rules to detect various network attacks.

• HOST BASED INTRUSION DETECTION SYSTEM - (HIDS)

→ HIDS ~~prefers~~ provides an additional security layer on imp sys like database servers

→ It watches activities on that specific machine to detect suspicious behaviour

→ It mainly:

- Detects intrusion
- Logs suspicous events
- Sends alerts
- Sometime stop attacks before damage happens

Date _____ Day _____

→ Can detect both internal & external attacks
→ NIDS or firewalls can't detect insider misuse
→ Detection methods
① Anomaly dections ② Signature detection
③ Heuristic (rule-based) detection

→ **Data Sources & Sensors used in HIDS**

① System Call Traces
- Records the sequence of sys call made by processes
- Works well on Unix/Linux
- Hard to see on Windows because DLLs (Dynamic Link Libraries) hide which process is calling what

② Audit (log) Records
- Logs collected automatically by the OS
- Advantage: No extra software needed
- Disadv:
  - ↳ Might not contain req info
  - ↳ Intruders may ~~hide~~ modify logs to hide their actions

③ File Integrity - Checksums
- Sys regularly compares imp files with "known good" checksum values
- Useful to see if an attacker changed any critical file

Date _____ Day _____

- Disadv:
  - ↳ Must protect original checksums
  - ↳ Hard to monitor, frequently changing files

(4) Registry Access (Windows)
- ↳ Watches changes & access to the Windows registry
- ↳ very specific to windows

Role of Sensor
- ↳ Collects data from these srces
- ↳ Cleans & format the data
- ↳ Sends it to the IDS analyzer

→ Anomaly HIDS
- ↳ Mostly anomaly-based HIDS is on Linux/Unix
- ↳ they mainly use system calls traces to detect abnormal process behaviour
- ↳ sys calls given detailed insights of OS & process interaction
- ↳ How it works?
  - ↳ Sys call sequences from current activity are compared with sequences from the training phase
  - ↳ Models used: Hidden Markov Model, Support Vector Machine

Date _____ Day _____

Artificial Neural Network, Extream Learning Machine

↳ ~~Earlier work~~

↳ Window HIDS

↳ Sys call tracing hard bcz DLLs

↳ Early attempts used audit logs or registry updates but low sucess

↳ Newer approach: Monitor DLLs func calls

↳ results similar to Linux HIDS

↳ Helps detect zero day attack

↳ Alternatives to Sys Call tracing

(1) Audit logs

(2) File-Integrity checking

↳ User cryptographic checksum

↳ limitations

↳ Cannot detect changes to runing processes

↳ Hard to pick which files to track

→ Signature Or Heuristic HIDS

↳ Commonly used in antivirus products

↳ Used on:

- Client systems
- Mobile devices
- Mail & web servers
- NIDS

Date _____ Day _____

↳ Signature-based: They match files against known malware signatures

↳ Heuristic-based: Use rules that describe typical malicious behaviour

↳ Very efficent at detecting known malware

↳ Cannot detect zero-day attacks

↳ Still heavily used, especially in Windows

→ Distributed HIDS

↳ Tradtional HIDS focus on a single systems

↳ Orgs have many hosts across a LAN → coordination is more effective than standalone HIDS on each host

↳ Key Design Issues:

① Diff data formats. — In a mixed env, host may use diff sensor → IDS must handle varying data

② Secure data transmission — Hosts sends sensor or audit data to analyzer. So integrity & confidentiality of that data must be mantained

③ Architecture Choice

↳ Centralized — One analysis center. Easy correlation but can be a bottle neck.

↳ Decentralized — more resilent, must coordinate & share info.

Date _____ Day _____

↳ Architecture

↳ three main components

① Host Agent Module

↳ Runs on each host

↳ Collects security-relevant events

↳ Sends to the centeral manager

② LAN Monitor Agent Module

↳ Monitors Network traffic

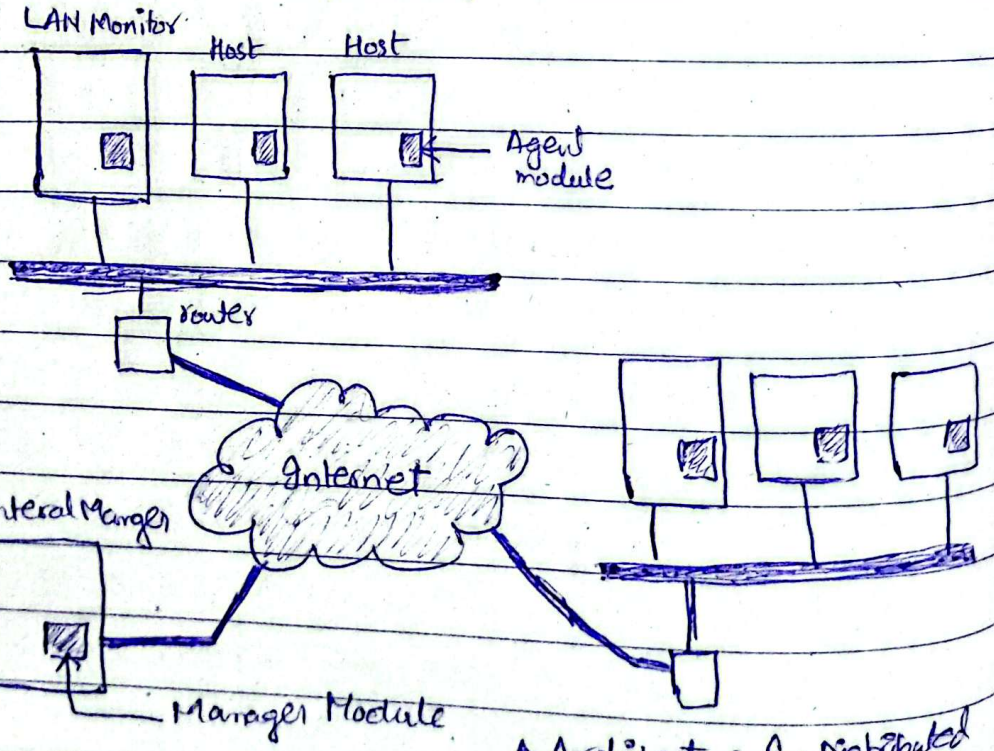
↳ Reports suspicious LAN activity to centeral manager

③ Centeral Manager Module

↳ Receives alert from all agents

↳ Correlates events

↳ Uses an expert sys to detect intrusions



▲ Architecture for Distributed Intrusion Detection sys

Page No. ☐

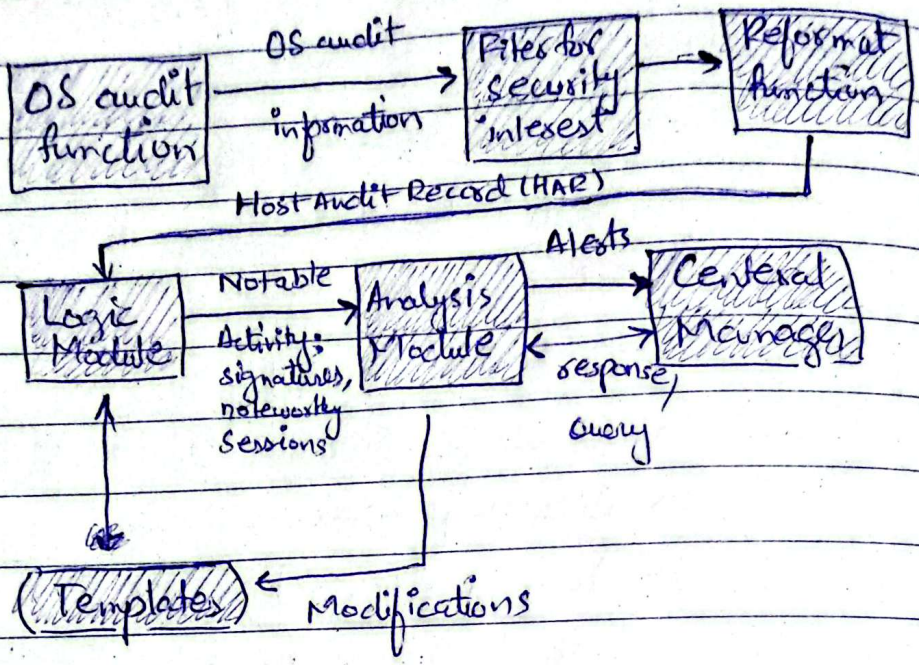
Date _____ Day _____

↳ Host Agent Hosting
- Captures native audit records
- Filters out only security-relevant records
- Converts them to a standard format : HAR
  ↳ Host Audit Record
- Uses templates to detect
  ↳ Single suspicious event (eg: failed file access)
  ↳ Attack patterns
  ↳ Anomalous user behaviour
- Sends alert to the central manager if suspicious activity detected

↳ LAN Monitor Agent Role
- Monitors → Host-to-host connections
  → Services being used
  → Traffic volume
- Detects → Sudden traffic changes
  → Use of sensitive services
  → Suspicious network activities

↳ Benefits
↳ Machine independent flexible design
↳ Allows correlation across multiple machines & networks
↳ Can detect intrusion that individual host alone could miss.

Date _____ Day _____



▲ Agent Architecture

● NETWORK BASED INTRUSION DETECTION

→ Monitors network traffic at selected points
→ Examines packets in real time to detect intrusion patterns
→ Looks at network, transport & application level activity
→ Usually part of the network's perimeter (boundary)
→ Mainly responsible for external intrusion detection
→ Analyzes both traffic pattern & content
→ Limitations
  ↳ Increasing use of encryption reduces content's visibility
→ NIDS Components
  ↳ Sensors ↳ Management Servers (Process alerts)
  ↳ Managment Consoles (Human Interface for monitoring)

Date _____ Day _____

→ Types Of Network Sensors

① Inline Sensors

↳ Placed directly inside the network path
↳ All traffic must pass through the sensors
↳ Often integrated with devices like firewalls or switches, or as a stand-alone inline NIDS
↳ Main Adv:
  ↳ Can block attacks immediately (intrusion detection + prevention)

② Passive Sensors

↳ Donot sit in the traffic path
↳ Monitor a copy of the network traffic
↳ More efficent — no added pkt delay
↳ Usually connected via fiber optic cable
↳ NIC (Network Interface Card) connected to cable has no IP Addr — only rcvs traffic
↳ A second NIC with an IP Addr sends alerts to the NIDS Management server

③ Wired vs Wireless Sensors

- Wired : Monitor traditional cable-based net traffic
- Wireless :
  ↳ Can be inline (built in Access Point) or passive
  ↳ Detects attack on wireless protocal
  ↳ Also called WIDS

Date _____ Day _____

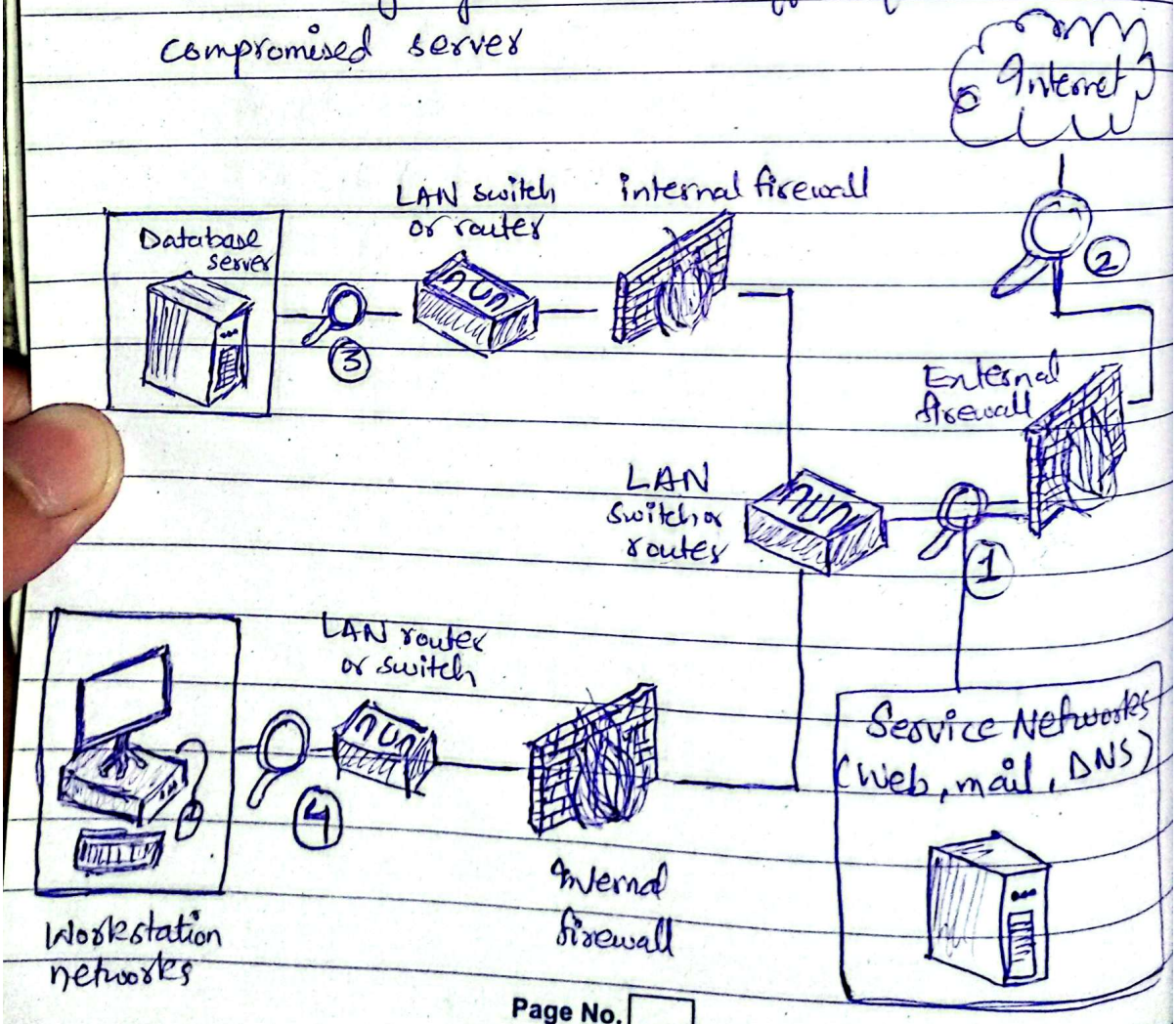
→ NIDS Sensor Deployment

↳ Large orgs with multiple sites & LANs need multiple NIDS sensors.

↳ Below are some sensor Placement options

(ii) Inside External Firewall

- Detects attacks that pass thru the external firewall
- Identifies firewall policy or performance issue
- Monitors attack on public facing server (Web, FTP)
- Even if an attack isn't detected, the IDS may detect outgoing malicious traffic from a compromised server



Date _____ Day _____

(2) B/w External Firewall & Internet / WAN

- Advantage
  - ↳ Sees all unfiltered traffic from the internet
  - ↳ Documents number & type of attacks targeting the network
- Disadv:
  - ↳ Has the highest processing load due to full traffic volume-

(3) Protecting Internal Backbone Networ.

- Monitors large traffic volumes → higher chance of spotting attack
- Detects internal misuse by authorised users
- Can be tuned to specific protocols or attacks
- Detects both internal & external attacks

(4) Protecting Department-Level or Critical LANS

- Used for sensitive networks (HR, Finance etc)
- Detects attack on critical sys
- Allows focusing security on high value assets
- Can be tuned to specific protocols & attacks.

Date _____ Day _____

→ Network Intrusion Detection Technique

↳ Uses two main methods, similar to HIDS

① Signature Detection

② Anamoly Detection

① Signature Detection

↳ Works by matching traffic against known attack patterns

↳ Examples:

↳ Application Layer Attack (HTTPS, FTP, DNS)

↳ Buffer overflow, pswd guessing, malware

↳ TCP layer

↳ unusual pkt fragmentation, port scanning SYN floods

↳ Network Layer

↳ IP Spoofing, illegal header val

② Anomaly Detection

Example:

↳ DoS

↳ Scanning

↳ Worms (unusual communication, new port usage)

Date _____ Day _____

- Stateful Protocol Analysis
  - ↳ A special type of Anomaly Detection
  - ↳ Compares traffic to trusted protocol behaviour profiles (from vendors)
  - ↳ Tracks protocol ~~steps~~ states to ensure the follows expected rules
  - ↳ Uses a lot of sys resources

→ Logging of Alerts

↳ Typical info logged by NIDS

- Timestamp
- Connection / session ID
- Event or alert type
- Rating
- Net, transport and app layer protocols
- Src & dest IP Add, Ports
- No. of bytes transmitted
- Decoded payload data
- State-related info

Date _____ Day _____

→ Centralize Adaptive Security Policy Sys

↳ A central sys starts with default security policy

↳ Recvs input from many distributed sensors across the network

↳ Based on these inputs it updates policy & sends instructions to devices

↳ The central sys makes decision based on 3 types of ~~events~~ events.

(1) Summary Events
- Collected from firewalls, IDS sys, servers
- These summarizes activity from parts of the network before they reach the central system

(2) DDI Events (Distributed Detection & Inference)
- Alerts generated by platforms through shared info
- They indicated platforms detected a possible attack

(3) PEP Events (Policy Enforcement Points)
- Comes from trusted platforms or advance IDS devices

Date _____ Day _____

- These systems correlate:
  - ↳ shared network info
  - ↳ local device decisions
  - ↳ host level actions

- Used to detect attacks that may not be visible on one single device.

↓

"Modern intrusion detection has moved towards coopesatived sys where many hosts & net devices acts as sensors, sharing info to detect attack faster & accurately.
This approach overcomes weakness of isolated IDS, which struggles to zero-day attacks.
Therefore a centralized sys is developed where each host or network is a node, a local detector which shares suspicions thru peer-to-peer "gossips" and when a threshold is reached (like enough no. of devices gives attack report) an attack is confirmed with lower false positives."

Mamroze