Network Security

* Comparison of IDS with Firewalls :-

→ Installing IDS and firewall offers cyber-security self to protect n/w.

→ IDS is a passive monitoring device that helps detects threat and generate alerts. An IDS provides no protection to the end-point

→ Firewall is an active protective device that is more like IPS. It performs analysis of the metadata of the n/w packets and helps block/allow the traffic based on some pre-set rules.

This creates a boundary on which some types of traffic ~~oo~~ or protocols cannot pass.

* Adv. of IDS :-

(i) It keeps a check on routers, firewalls, key servers and files and uses its database to raise the alarm & send notifications.

(ii) offers centralized management for the correlation of the attack.

(iii) It analyzes diff. attacks, identifies their patterns and helps the administrater to organize and implement effective control.

(iv) Acts as additional layer of protection for the company.

* Disadv. / Challenges of IDS :-

(i) Ensuring Effective Deployment :-

→ Deploying IDS can be tricky, and if not done properly it may create vulnerabilities for critical assets.

(ii) Understanding and Investigating Alerts :-

→ IDS alerts gives very little info. which is sometimes hard to investigate.

→ Also, investigating the IDS alerts can be time and resource-intensive, which may require additional info. to identify the seriousness of the attack.

(iii) Managing a High volume of Alerts :-

→ Since, there is vast majority of attacks are generated by IDS, it may put burden on internal teams to identify each of them.

(iv) Knowing How to Tackle Threats :-

→ Sometimes a home IDS gives false alarms, so cyber security team needs to be updated with latest updates in IDS and key domains of cyber security.

* IPS (Intrusion Prevention System) :-

→ IPS is also known as Intrusion Detection and Prevention System.

→ Major function of IPSs are to identify malicious activity, collect info. about this activity, report it and attempt to block or stop it.

→ IPSs are contemplated as argumentation of IDS because both operate n/w traffic and system activities for malicious activity.

→ IPS typically record info. related to observed events, notify security administrators/

and produce reports.

→ Many IPS also respond to threats by attempting to prevent it from succeeding.

→ They use various response techniques which involve the IPS stopping the attack itself.

* Classification :-

4-types

1. Network-Based Intrusion prevention System (NIPS) :-

→ It moniters the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless IPS (WIPS) :-

→ It moniters wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network Behaviour Analysis (NBA) :-

→ It examines n/w traffic to identify threats that generates unusual traffic flows, such as distributed denial of service attacks, speific form of malware & policy violations.

4. Host-Based IPS (HIPS) :-

→ It is an inbuilt s/w package which operates a single host for doubtful activity by scanning events that occur within that host

* Detection method of IPS :-

1. Signature-Based Detection :-

→ It operates packets in n/w and compares with pre-built and predefined attack patterns known as signatures.

2. Statistical anamaly-based Detection :-

→ It monitors n/w traffic and compares it against an established baseline.

→ The baseline will identify what is normal for that n/w and what protocols are used.

→ However, it may raise a false alarm if the baseline is net intelligently cofigured.

~~3. Stateful protocol analysis detection :-~~

3. Policy-Based detection :-

→ It requires system administrators to cofigure security policies based on an organization's security policies and n/w infrastructure.

→ If any activity breaks a defined security policy, an alert is triggered and sent to the admin's.

* Comparison of IPS with IDS :-

→ IDS is more of a alerting system that lets an organization know if anamalous or malicious activity is detected.

An IPS takes this detection one step further and shuts down the n/w before access can be gained or to prevent further movement in a n/w.

4

Date
Page

* **Audit Trail :-**

→ Audit trail keeps track of different action that took place for an activity in an chronological order.

→ Therefore, the audit trail records :-

- who : user or appl^n program and a transaction no.
- when : Date and Time
- where : location of user
- what : Data that is being worked upon or is modified.

→ e.g, when checkout from the counter of a market after shopping, the bill is type of audit trail, where we fill all necessary info.

* **Why Audit Trail :-**

→ Audit Trail is one of the most essential thing for any company or organization as they keep track of all the things and any chaos / irregularity in the future can be rectified.

→ It enhances security of an organization.

→ It makes an organization trustworthy.

→ All types of industries and organizations makes it mandatory to maintain an audit trail as they deal with sensitive info. and data.

* **Types of Audit Trail :-**

1 **External Audits :-**

→ An external audit is an independent examination of the financial statements prepared by the organization.

→ External audits are performed by CPA(certified public accountants) firms hired by a business. to ensure correctness and acuracy of accounding records maintained by a company.

2. Internal Audits :-

→ They are performed within the organization, one department performs audit for other department

→ This helps in growth of an organization and take actions for further growth and steps to avoid upcoming risk.

3. Internal Revenue Service (IRS) Audit :

→ Performed to avoid any tax violations.

→ It is a type of external audit performed on organizations that are acused guilty of providing wrong tax data.

* Advantages :

1. Fraud Preventions.
2. Easy verification
3. Maintaining Financial History.
4. Easy recovery.

* Disadvantages :

1. Maintainance cost :

→ extra maintainance that it requires, hiring of CA, cost of memory etc.

2. Security threats :-

→ The audit trails are taken care of but if fall in hands of a attack all data of a company will be leaked.