SMVS
Page No.
Date : / /

Access Control and Intrusion Detection

* Authentication and Authorization

	Authentication	Authorization
1	Verifying the identity of a user.	Determining the user's access levels.
2	Confirms if the user is who they claim to be.	Specifies what resources the user is allowed to use.
3	Involves crediantial like username or Password.	Involves checking policies, rules to follow by users.
4	First, before Authorization.	After the complete Authentication.
5	Visible to the user	Not visible to the user.
6	Control by the user	Control by the system.
7	Implemented via Login system.	Implemented via role-based access.

* Intrusion, Intrusion Detection System with Feature.

=> Intrusion refers to the act of gaining unauthorized access of a device, network or system.

Attacker use different method to perform Intrusion in the system.

=> Intrusion Detection System:

Intrusion Detection System is used to detect the intrusion in the system.

-> Working of IDS:

1 Traffic Monitoring: The IDS monitors network traffic or host activity.

2 Data Analysis: It analyzes data flowing through the network to find patterns.

3 Rule Comparison: The system compare network or host activity

SMVS
Page No.
Date : / /

against a set of predefined rules.

4 Attack
4 Alert Generation : When the IDS detects activity that matches know attack signature than it generates alert.

5 Administrator Response : The system administrator receive the alert and take action against attack

⇒ Classification of IDS :

1 Network Instrusion Detection System :

- NIDS is set up at strategic points within the network to monitor traffic across all devices.

Observes traffic on the entire subnet and matches it to known attack pattern.

Ideal for monitoring network-wide traffic and detecting threats at network level.

SMVS
Page No.
Date : / /

2 Host Instruction Detection :

HIDS installed on individual hosts or devices.

HIDS monitores incoming and outcoming packets From the specific device.

Effective For protecting individual devices and detecting local attacks.

3 Protocol-Based (~~local~~) IDS:

PIDS positioned at the Front end of a server to monitor and interpret protocol traffic.

Monitors HTTPS traffic before it reaches the web server.

Ensures security by focusing on the integrity of communication protocols.

4 Application Protocol-Based IDS:

APIDS operates within groups

SMVS
Page No.
Date : / /

of servers, focusing on application specific protocols.

Monitors and interprets traffic related to specific application such as SQL.

5 Hybrid Instruction Detection System:

HIDS combines elements of multiple IDS types.

Provides a more complete threat detection system by merging different approaches.

=> IDS Features:

1 Real time data Monitoring on network.

2 Signature-Based detection

3 Anomaly Detection

4 Alerting and Reporting of Instruction

5 Integration with Other Security Tools

6 Logging and Data Collection

7 Customizable Rules and Policies

8 Scalability

* Intrustion Prevention System:

=> Intrusion Prevention System are security tool designed to detect and prevent threats and attack in real time.

-> IPS Works:

1 Traffic Inspection: Continuously examines network or system traffic

2 Detection and Prevention: Uses detection methods to identify threats and take action to prevent them.

3 Policy Enforcement: Applies predefine security policies and rules to manage and control access.

SMVS
Page No.
Date : / /

4 Response Actions: Automatically blocks or mitigates threat based on configured response actions.

5 Logging and Alerts: Records events and generates alert for administrators to review and investigate.

=> Classification of IPS:

1 Network-based Intrusion Prevention System:

Monitors and analyzes traffic across the entire network to detect and prevent malicious activities.

Analyzes network and generates alerts for detects threats and can take automated action like blocking traffic.

2 Wireless IPS:

Specifically designed to monitor and protect wireless networks from unauthorized access and attacks.

Identifies and mitigates interference from non-network sources that disrupt wireless communication.

3 Network Behavior Analysis

Analyzes network traffic patterns and flow to identify unusual behavior.

Identifies and alerts on violation of network policies such as unauthorized access attempts.

4 Host-Based IPS:

HIPS operates on individual hosts to monitor and protect the host from malicious activity.

Monitors and compare system file and configuration to detect unauthorized changes or tampering.

=> Features of IPS:

1 Real-time Threat Prevention

SMVS
Page No.
Date : / /

2 Active Response Mechanism

3 signature-Based Detection

4 Anomaly Detection

5 Protocol Analysis

6 Integration with other security solution

7 Customizable Policies and Rules.