R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contentsof this informationisstrictlyprohibited.

22CS930 ENTERPRISE CYBER SECURITY

Department: CSE(CS)

Batch/Year: 2022-2026/IV

Created by: Dr. Udhaya Sankar S M

Date: 15.5.2025

1.TABLE OF CONTENTS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

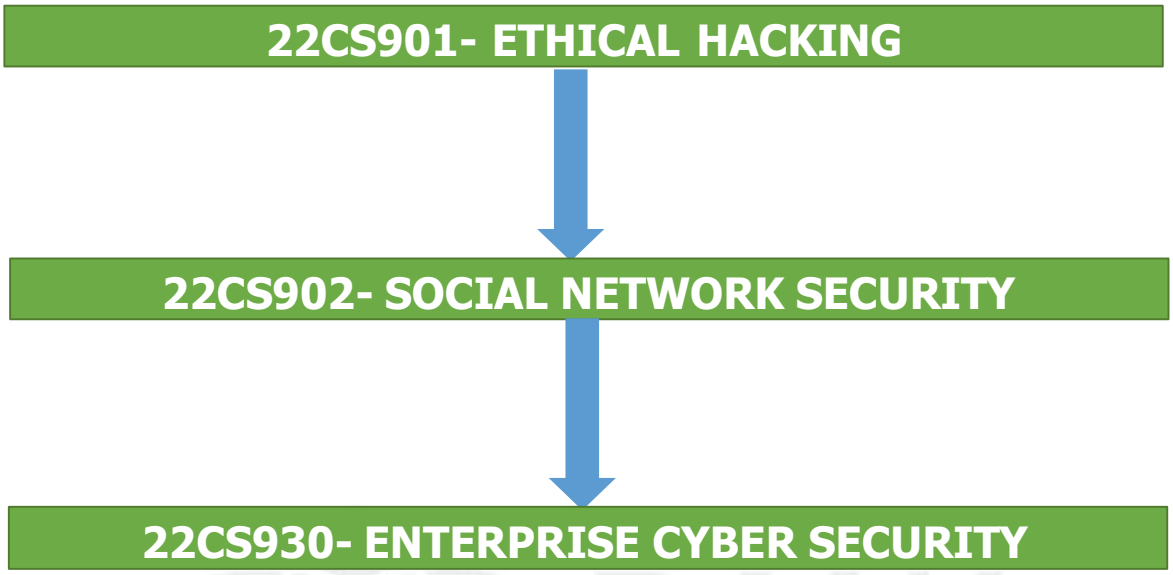
2. COURSE OBJECTIVES

- Learn the fundamentals of cryptography.
- Learn the key management techniques and authentication approaches.
- Explore the network and transport layer security techniques.
- Understand the application layer security standards.
- Learn the real time security practices.

R.M.K GROUP OF INSTITUTIONS

3. PRE REQUISITES

PRE-REQUISITE CHART



R.M.K GROUP OF INSTITUTIONS

4.SYLLABUS

22CS930- ENTERPRISE CYBER SECURITY

L T P C
3 0 0 3

Unit-I INTRODUCTIONTOCYBERSECURITY 9

Cyber Security – Need of Cybersecurity in Organizations – CIA Triad- Confidentiality, Integrity, Availability; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes– A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

Unit II : NETWORK SECURITY BASICS 9

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

Unit III : SECURE COMMUNICATION PROTOCOLS 9

Encryption Principles- Cryptography, Cryptanalysis, Feistel Cipher Structure. Block Encryption algorithms: DES, triple DES, and AES. Transport-Level Security: Secure Sockets Layer (SSL), Transport Layer Security TLS). Electronic Mail Security- Pretty Good Privacy (PGP), S/MIME. Securing wireless networks: WPA, WPA2, WPA3.

Unit IV : INTRUSION DETECTION AND PREVENTION SYSTEMS 9

IDPS- Need of Intrusion Detection Systems in Cyber Security- Types of IDPS: Network-based and Host-based. Configuring and Managing IDPS for threat detection using Honeypots. Case Study: Setup a honey pot and monitor the honey pot on network.

Unit V : WEB APPLICATION SECURITY 9

Introduction to Web Application Vulnerabilities – Cross Site Scripting (XSS) – SQL injection- Denial of Service (DoS)- Web Application Testing - Types of Penetration Tests- OWASP and OWAS9P Top.

R.M.K GROUP OF INSTITUTIONS

5.COURSE OUTCOME

Course Code	Course Outcome Statement	Cognitive / Affective Level of the Course Outcome	Course Outcome
Course Outcome Statements in Cognitive Domain			
22CS930	Understanding the core concepts and importance of cybersecurity in organizational settings.	Understanding K2	CO1
22CS930	Acquire the knowledge common network attacks and deploy appropriate security measures.	Apply K3	CO2
22CS930	Implement encryption and secure communication protocols for data integrity and confidentiality.	Apply K3	CO3
22CS930	Deploy and manage Intrusion Detection and Prevention Systems for threat detection.	Analyse K4	CO4
22CS930	Identify and mitigate common web application vulnerabilities.	Analyse K4	CO5
22CS930	Conduct penetration tests to evaluate the security posture of web applications.	Evaluate K5	CO6

6.CO-PO/PSO MAPPING

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes.

Course Outcome COs	K-Levels	Program Outcomes(POs) , Program Specific Outcomes (PSO)												
		PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO2
22CS930.1	K2	3	2	-	-	-	-	-	-	-	2	-	-	3	-
22CS930.1	K3	3	3	2	-	-	-	-	-	-	2	-	1	3	2
22CS930.1	K3	3	3	3	2	2	-	-	-	-	2	-	2	3	3
22CS930.1	K4	3	3	3	2	2	-	-	-	-	2	-	2	3	3
22CS930.1	K4	3	3	3	-	-	-	-	-	-	2	-	2	3	3
22CS930.1	K5	3	3	3	2	2	-	-	-	-	2	-	2	3	3

UNIT IV
INTRUSION DETECTION AND PREVENTION SYSTEMS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

7.LECTURE PLAN – UNIT IV

UNIT IV -INTRUSION DETECTION AND PREVENTION SYSTEMS							
SNo	Topics	No. of Periods	Poposed Lecture period	Actual Lecture period	Pertaining COS	Taxonomy Level	Mode of Delivery
1	IDPS- Need of Intrusion Detection Systems in Cyber Security	1			CO4	K2	MD1, MD5
2	Types of IDPS: Network-based and Host-based.	1			CO4	K4	MD1, MD5
3	Configuring and Managing IDPS for threat detection using Honeypots.	1			CO4	K3	MD1, MD5
4	Case Study: Setup a honey pot and monitor the honey pot on network.	1			CO3	K4,K5	MD1, MD5

R.M.K GROUP OF INSTITUTIONS

7. LECTURE PLAN – UNIT IV

ASSESSMENT COMPONENTS

- AC 1. Unit Test
- AC 2. Assignment
- AC 3. Course Seminar
- AC 4. Course Quiz
- AC 5. Case Study
- AC 6. Record Work
- AC 7. Lab / Mini Project
- AC 8. Lab Model Exam
- AC 9. Project Review

MODE OF DELEIVERY

MD 1. Oral presentation
MD 2. Tutorial
MD 3. Seminar
MD 4 Hands On
MD 5. Videos
MD 6. Field Visit

R.M.K GROUP OF INSTITUTIONS

8 ACTIVITY BASED LEARNING : UNIT – IV

ACTIVITY 1: Integrated Activity-Based Learning Plan

Objective:

Setup a Honeypot and Monitor

Activity Overview

- Students will be divided into teams. Each team will simulate a Configuration and Monitoring of Intrusion Detection Systems (IDPS) using Honeypots for Threat Analysis
- Environment Setup:

  Use Kali Linux or Ubuntu VM.

  Install Cowrie honeypot (SSH/Telnet fake server).
- Configuration:

  Redirect traffic to honeypot port (e.g., 22 for SSH).

  Configure logging for all connections and commands.
- Monitoring:

  Capture attacker IPs, login attempts, and executed commands.

  Monitor with ELK Stack (Elasticsearch + Kibana) for visualization.
- Analysis:

  Identify repeated brute force attempts.

  Extract malware samples if uploaded by attacker.

  Compare with IDPS logs to validate detection.

R.M.K GROUP OF INSTITUTIONS

9 LECTURE NOTES : UNIT – IV
INTRUSION DETECTION AND PREVENTION SYSTEMS

1. IDPS- Need of Intrusion Detection Systems in Cyber Security

Intrusion detection refers to the process of monitoring activities within a computer system or network and analyzing them for signs of potential security incidents. These incidents may involve violations or threats of violating security policies, acceptable use policies, or standard security practices. Intrusion prevention builds on detection by taking proactive measures to stop detected threats.

Intrusion Detection and Prevention Systems (IDPS) are designed to identify potential incidents, log details about them, attempt to block malicious activities, and alert security administrators. Beyond these functions, organizations also use IDPSs to evaluate security policies, track known threats, and discourage policy violations.

Needs for IDS in Cybersecurity

Threat Detection – Identifies unauthorized or suspicious activities such as abnormal logins or malware behavior.

Real-time Alerts – Immediately notifies system administrators when potential intrusions are detected.

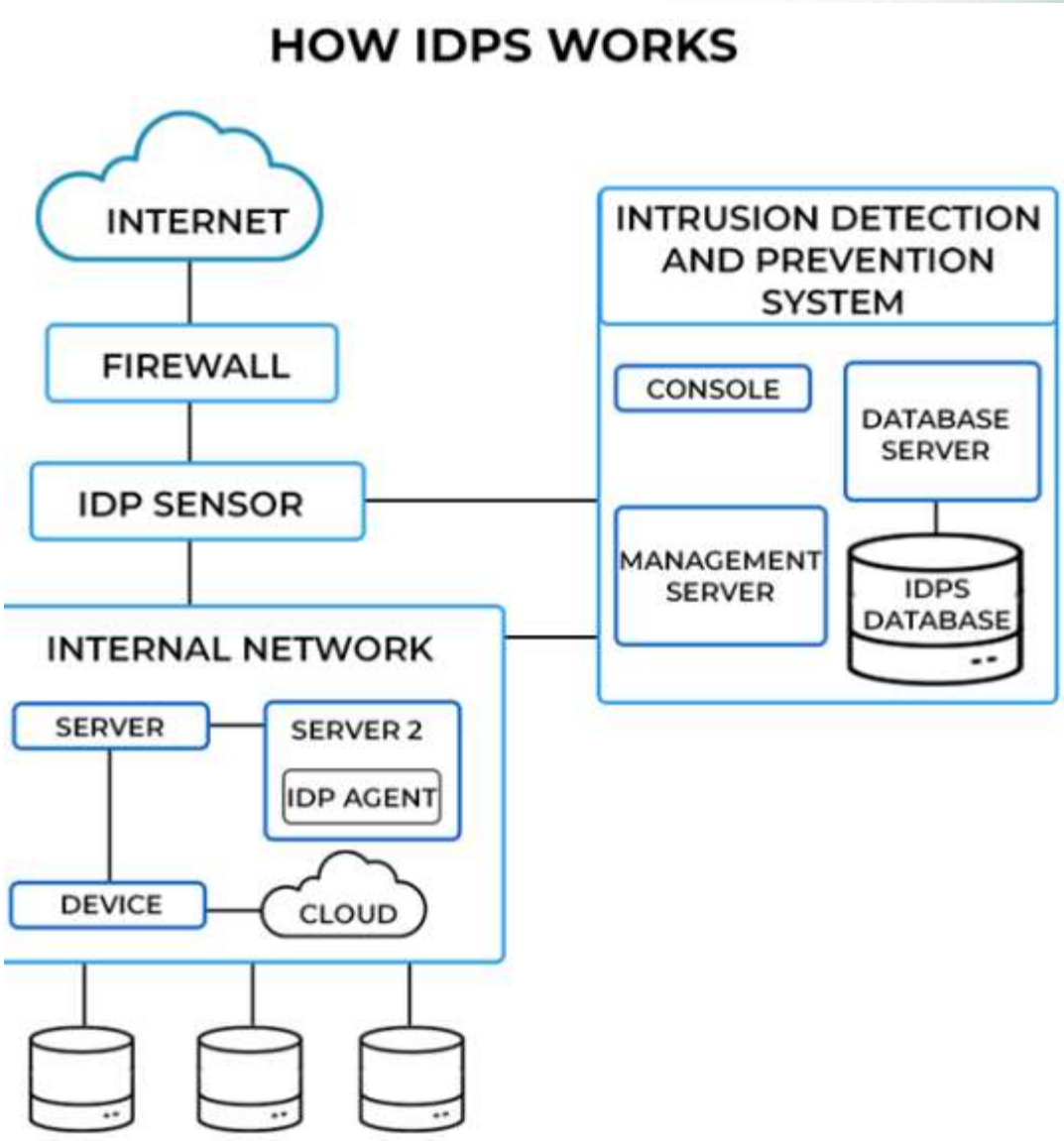
Network Monitoring – Continuously observes traffic and system activities for unusual patterns.

Policy Enforcement – Helps ensure adherence to security policies by detecting violations.

Incident Response Support – Provides detailed logs and forensic data for investigating attacks.

Protection Against Insider Misuse – Detects suspicious actions carried out by internal users.

Minimizing Impact – Enables early detection of intrusions, reducing the potential damage or downtime.



An Intrusion Detection and Prevention System (IDPS) works by monitoring network traffic and system activities to detect suspicious behavior. It analyzes data using signature-based detection (matching known attack patterns) or anomaly-based detection (spotting unusual activity). When a threat is found, the IDPS logs it, alerts administrators, and can respond either passively by reporting or actively by blocking malicious IPs, dropping harmful packets, or reconfiguring firewalls. It also generates reports to improve security policies and future detection.

2.TYPES OF IDPS

Host-based Intrusion Detection System

A Host-based Intrusion Detection System (HIDS) is a security mechanism designed to monitor and analyze the internal state of a computer or server for malicious or unauthorized activities. Unlike Network-based Intrusion Detection Systems (NIDS), which focus on monitoring traffic flowing across a network, HIDS provides visibility into what is happening within a specific host. It collects and analyzes data such as system calls, log files, file integrity, and user activities to detect suspicious behavior.

A Host-based Intrusion Detection System (HIDS) treats the host as an independent environment, whether it is a personal computer or a server. Its primary function is to analyze and monitor the internal activities of that system. It operates by examining files and data entering or leaving the host. The system works by capturing a snapshot of the current file system and comparing it with a previously recorded snapshot. If both remain identical, the host is considered secure; however, any discrepancies may indicate a potential intrusion or attack.

With the rapid rise of malware, ransomware, insider threats, and advanced persistent threats (APTs), HIDS has become a critical component of modern cybersecurity. It not only identifies intrusions but can also provide forensic evidence for security investigations.

The architecture of a typical HIDS includes several components:

Data Sources

Operating system event logs.

Application logs (web server logs, database logs).

System files and configuration files.

User authentication logs.

R.M.K GROUP OF INSTITUTIONS

Data Collection Agent

Installed on the host machine.

Continuously gathers relevant system data.

Analysis Engine

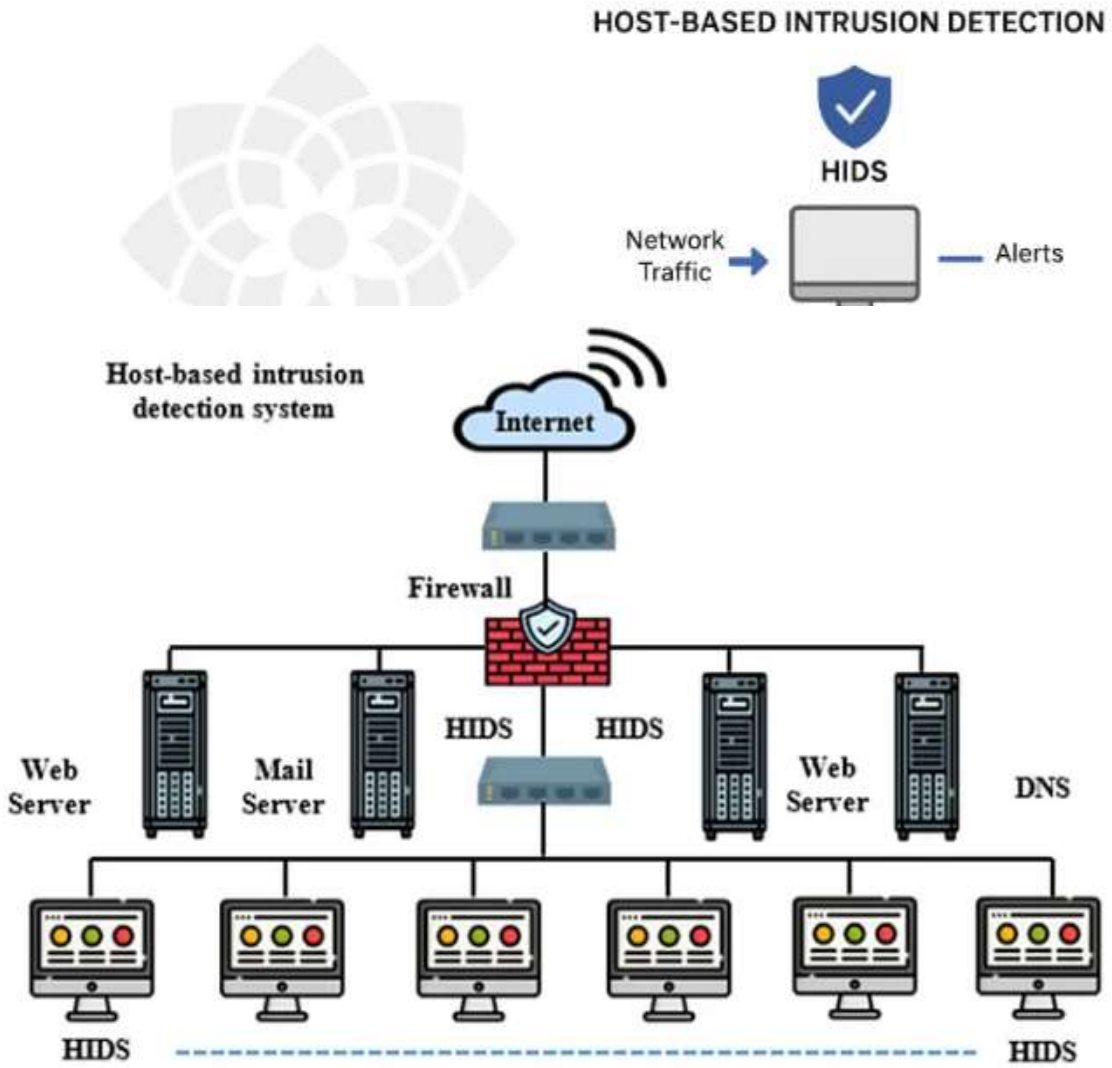
Compares collected data against known attack signatures.

Detects deviations from normal behavior.

Alerting and Reporting Module

Generates alerts when suspicious activity is detected.

Stores events in a database or forwards them to a Security Information and Event Management (SIEM) system.



Detection Techniques in HIDS

HIDS employs several techniques for detecting intrusions:

Signature-based Detection

Matches system activity against a database of known attack patterns. For example, if a log entry matches a known brute-force attack signature, an alert is triggered.

Anomaly-based Detection

Establishes a baseline of normal system behavior (CPU usage, system calls, login patterns). Any deviation from this baseline may indicate an attack.

Heuristic Detection

Uses rule-based logic or AI to detect previously unknown threats.

Hybrid Detection

Combines signature and anomaly methods for better accuracy.

HIDS' advantages:

In-depth monitoring and log analysis

Being independent of network architecture

File integrity monitoring

Detecting local incidents

Real-time alerts[6]

HIDS' disadvantages:

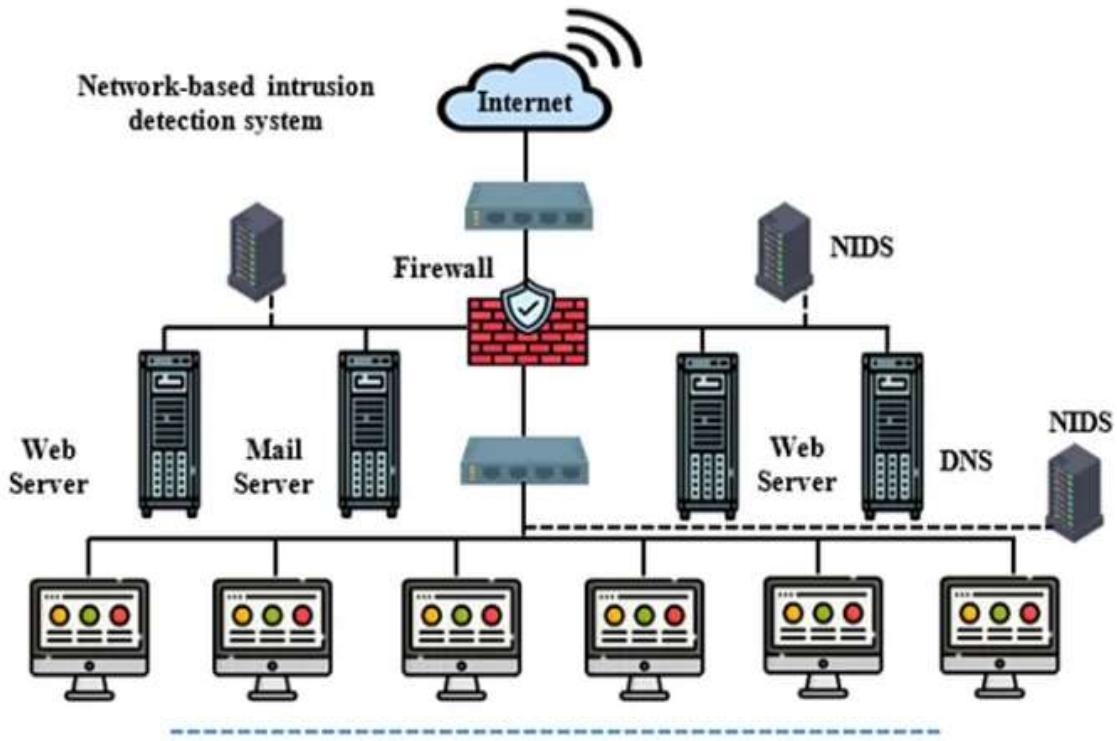
It can be resource intensive for hosts

It can only monitor the host, not the whole network[6]

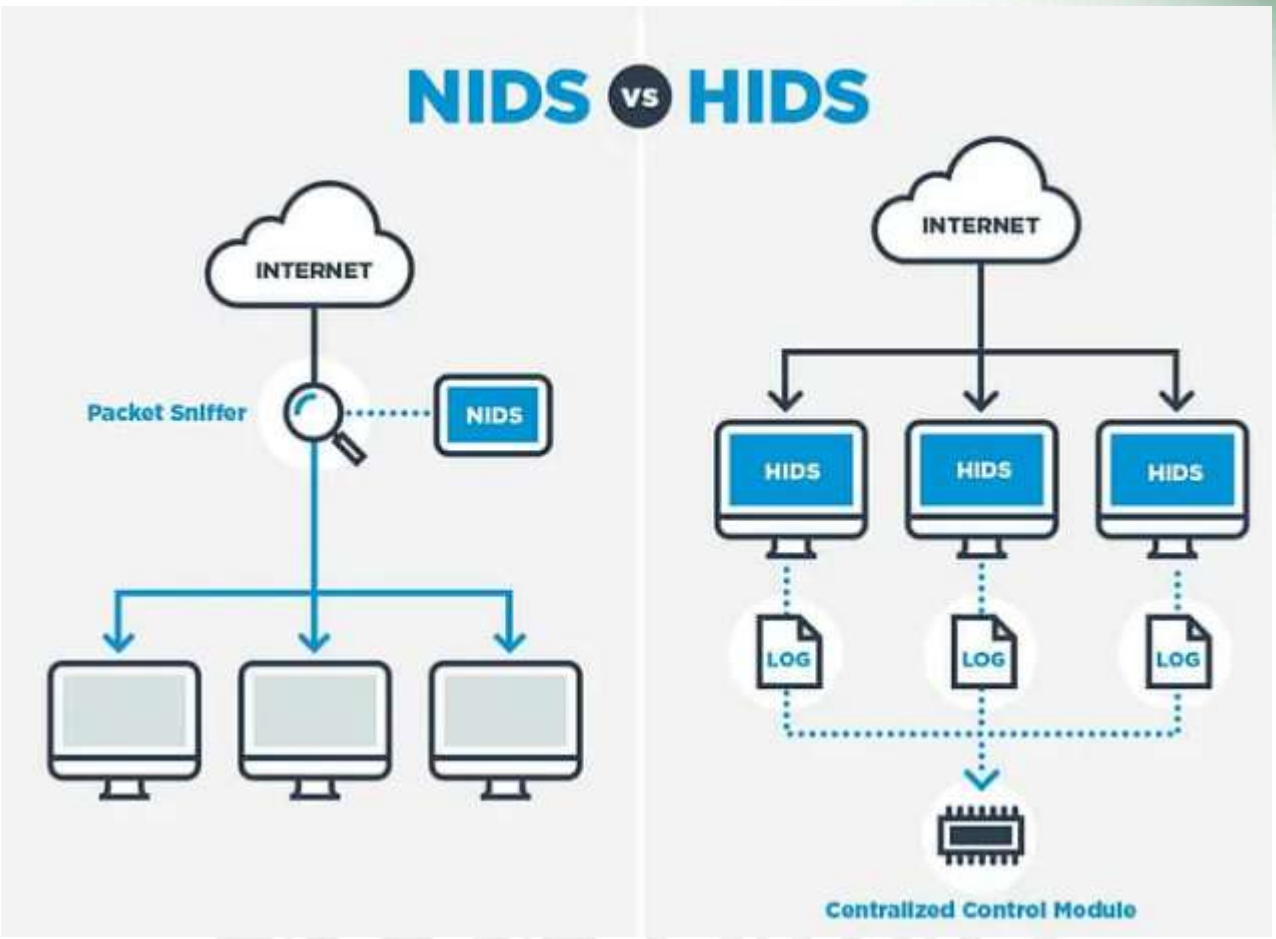
R.M.K GROUP OF INSTITUTIONS

Network-based Intrusion Detection System

A Network Intrusion Detection System (NIDS) is a security mechanism designed to monitor and analyze network traffic in real-time to detect suspicious activities, cyberattacks, or policy violations. It is typically deployed at strategic points within the network, such as routers, firewalls, or gateways, where it can capture and inspect data packets moving across the system. NIDS operates using two main detection techniques: signature-based detection, which compares network traffic against known attack patterns, and anomaly-based detection, which identifies unusual behavior that deviates from normal network activity. By providing real-time alerts and maintaining logs of network events, NIDS helps administrators quickly respond to potential threats like denial-of-service (DoS) attacks, port scans, malware, or unauthorized access attempts. Although NIDS offers wide visibility across the entire network and is effective against many external threats, it has limitations such as difficulty inspecting encrypted traffic, the risk of false positives, and performance challenges in high-traffic environments. Popular examples of NIDS include Snort, Suricata, and Zeek (formerly Bro).



R.M.K GROUP OF INSTITUTIONS



Feature	NIDS	HIDS
What it monitors	Network traffic	System logs, file integrity, processes on a host
Where it is deployed	At network transit points or segments	On individual servers and endpoints
Primary role	Detecting network-wide attacks	Detecting internal attacks and host-specific compromises

R.M.K GROUP OF INSTITUTIONS

Categories	HIDS (Host Intrusion Detection System)	NIDS (Network Intrusion Detection System)
Definition	Monitors a single host for suspicious activity	Monitors the entire network traffic
Type	Does not work in real-time	Works in real-time
Concern	Focused on a single host system	Focused on the entire network
Installation Point	Installed on each host/server	Installed at network points like routers or gateways
Execution Process	Compares current system snapshot with stored malicious patterns (delayed)	Analyzes traffic in real-time and reports anomalies
Information About Attack	Provides detailed information about attacks (system-level files/processes)	Less detailed, as it focuses on overall traffic flow
Ease of Installation	Complex, needs installation on every host	Easier, fewer installation points
Response Time	Slow response	Fast response

R.M.K GROUP OF INSTITUTIONS

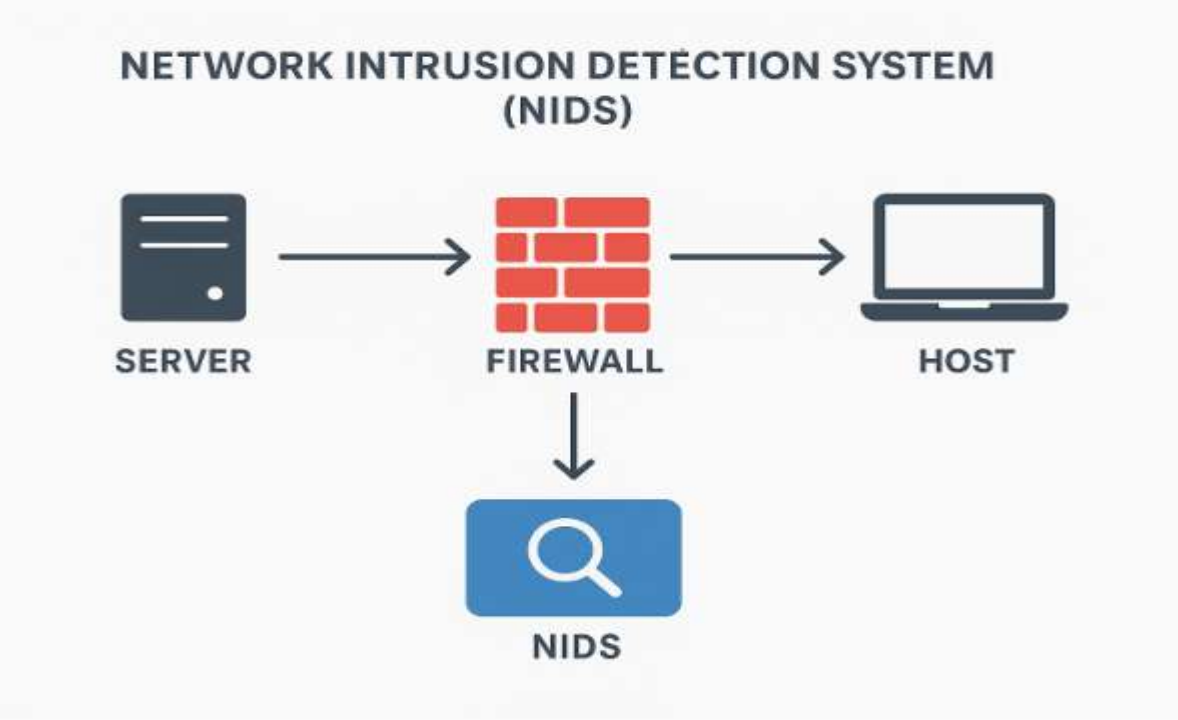
The biggest differences between NIDS and HIDS:

Focus and scope (HIDS focuses on individual hosts while NIDS monitors the whole network)

Location and data collection (HIDS is installed on individual hosts and collects local logs while NIDS is deployed at a strategic point in the network to monitor outgoing traffic and look for anomalies)

Place of Detection (HIDS uses signature- & anomoly based detection directly on the host while NIDS uses signature- & anomaly-based detection across the entire network)

Resource utilization and scalability (HIDS can be resource intensive on hosts while NIDS monitors centrally which reduces impact on individual hosts)[6]



Network-Based Intrusion Detection System (NIDS)

NIDS monitors the entire network by analyzing traffic and data flow in real-time. It is typically installed at strategic points like routers or servers to oversee network-wide activities. NIDS excels in detecting attacks across multiple systems and does not impact the performance of individual hosts. However, it may struggle with encrypted traffic and can be slower due to the volume of data it processes.

Advantage of NID

Detect attacks in the entire network

It can use the information collected from attacks on different hosts to detect attacks on a new or fresh host.

Host production/performance remains unaffected.

Disadvantage of NID

It might be slow as compared to the network speed.

Scrutinizing protected channels may possess difficult.

It is also passive in nature.

R.M.K GROUP OF INSTITUTIONS

3. Configuring and Managing IDPS for threat detection using HoneyPot

In cybersecurity, honeypots are decoy systems or servers placed alongside an organization's real production systems. They are intentionally designed to appear as valuable targets, luring attackers away from critical resources. By engaging with the honeypot, attackers reveal their tactics while IT teams gain the opportunity to monitor security responses and analyze malicious activity without jeopardizing actual assets.

Different types of honeypots can be deployed depending on organizational needs. Since they mimic legitimate systems, they serve as traps that help detect attacks early, gather intelligence about the intruder's methods, and respond effectively. For maximum effectiveness, a honeypot should resemble a genuine production system by running similar processes and containing realistic-looking decoy files.

In many setups, honeypots are positioned behind the organization's firewall. This allows them to capture threats that bypass perimeter defenses while preventing compromised honeypots from being used to launch further attacks. As attacks unfold, the firewall acts as a safeguard between the honeypot and the internet, intercepting malicious traffic and neutralizing potential risks.

Working of Honeypot

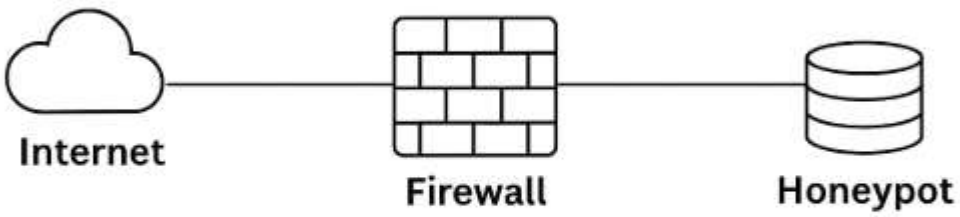
A honeypot works by mimicking a genuine computer system, complete with applications and data that cybercriminals typically seek out. For example, it may be designed to resemble a server holding sensitive customer information, such as credit card numbers or personal identification data. To make it convincing, the system is filled with decoy information that appears valuable to an attacker.

Once an intruder attempts to breach the honeypot, security teams can closely observe their methods, track the tools and techniques they use, and assess how the system's defenses respond. This intelligence can then be used to strengthen the organization's overall security posture.

Honeypots deliberately contain vulnerabilities to attract attackers. They may, for instance, have open ports that appear exploitable during a port scan. By engaging with these seemingly weak points, attackers unknowingly allow the security team to study their approach and behavior.

Unlike traditional security tools that directly block attacks, honeypots are designed to analyze threats rather than prevent them outright. Their purpose is to enhance intrusion detection systems (IDS) and improve incident response strategies, ensuring the organization is better

BASIC HONEYPOT DIAGRAM



A honeypot network configures and deploys additional resource that appears to be a source of traffic originating from them. Internet traffic to the adversaries to disguise by disguising itself a a possible target.

Different Types of Honeypots and How They Work

Malware Honeypot

Malware honeypots are designed to attract malicious software by emulating known attack vectors. For example, they may simulate a Universal Serial Bus (USB) storage device. When malware attempts to infect the emulated USB, the honeypot captures its behavior, allowing researchers to study how it operates.

Spam Honeypot

Spam honeypots trick spammers by posing as open proxies or mail relays. Spammers often test mail relays by sending themselves emails; if successful, they use them to distribute large volumes of spam. A spam trap detects these test attempts and can block the spammer's activity.

Database Honeypot

Database honeypots are decoy databases created to lure attackers targeting structured data with techniques like SQL injections. These honeypots can be combined with database firewalls to study attempts at unauthorized data manipulation.

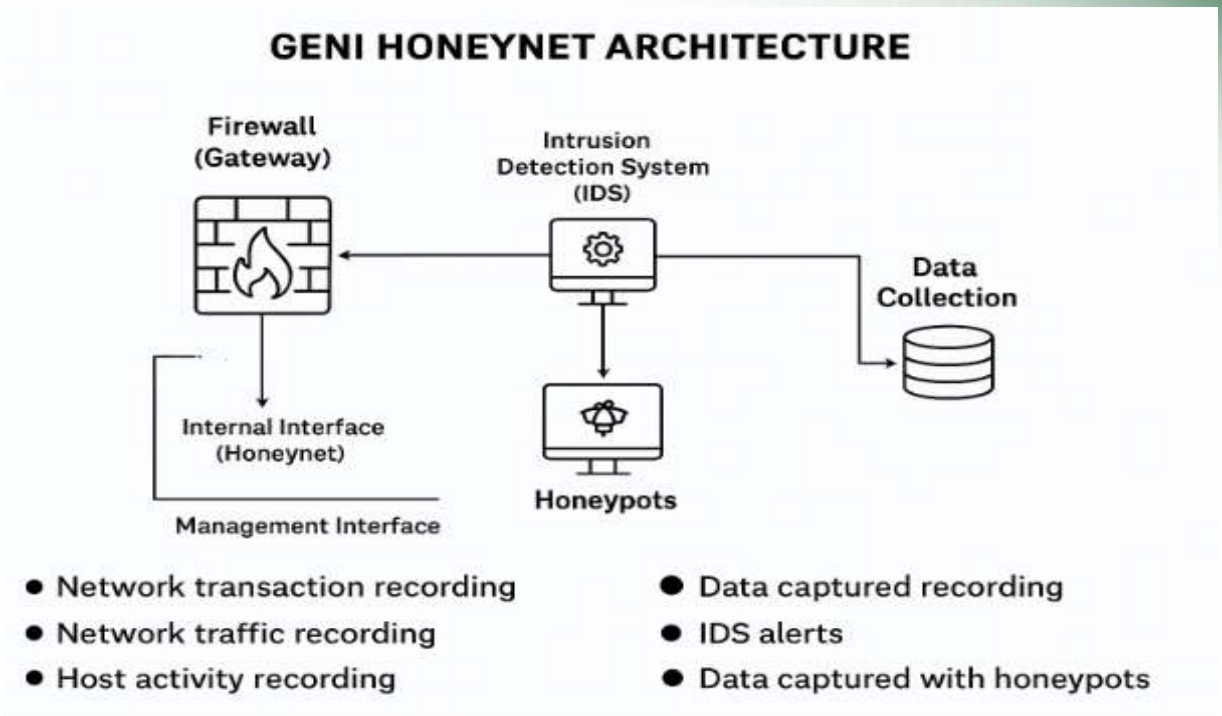
Client Honeypot

Client honeypots mimic client systems to attract malicious servers controlled by attackers. They pretend to be a legitimate client and observe how the attacker manipulates the server during the intrusion. Typically, client honeypots run in virtualized environments with safeguards to minimize exposure risks.

Honeynet

A honeynet is a collection of interconnected honeypots designed to study multiple types of attacks simultaneously. Honeynets can analyze distributed denial-of-service (DDoS) attempts, ransomware campaigns, or CDN-targeted exploits. They are configured to contain all inbound and outbound traffic, ensuring the rest of the organization's systems remain safe.

R.M.K GROUP OF INSTITUTIONS



The GenI Honeynet Architecture is designed as a controlled and monitored environment to study attackers' behaviors without putting the production network at risk. It relies on three main components: Firewall, Intrusion Detection System (IDS), and Data Collection Framework.

1. Firewall (Gateway)

The firewall is the frontline defense and acts as a traffic manager for the honeypot network.

Purpose: It isolates the honeynet from the external (real) network and ensures controlled interaction.

Interfaces:

External Interface (Network): The entry point for all inbound traffic from the internet into the honeynet.

Internal Interface (Honeynet): Connects the firewall to the honeypot systems inside the honeynet.

Management Interface: Used only for administrative purposes, such as extracting logs, configuring rules, and monitoring activity.

Functions:

Works as a security guard, deciding which packets are allowed to et.

R.M.K GROUP OF INSTITUTIONS

Traffic shaping: Controls the rate and amount of data passing through to prevent flooding.

oBlocking malicious connections: Stops unauthorized or suspicious communication.

oPrevents compromised honeypots from launching outbound attacks on real networks.

2. **Intrusion Detection System (IDS)**

The IDS continuously monitors honeynet traffic for suspicious patterns, unusual behavior, or malicious attempts.

•**Components:**

Management Interface (with IP address): Connected to the production/admin network for log collection, alerts, and system configuration.

Monitoring Interface (no IP address): Connected passively to a router or switch port. It silently observes all traffic without being detectable by attackers.

•**Functions:**

Captures traffic going to and from honeypots.

Logs network activities such as communication endpoints, protocols, and payloads.

Monitors host activity (honeypot behavior).

Generates alerts for suspicious or malicious activities detected.

Limitation: Since IDS relies mainly on network-level traffic inspection, attackers may attempt evasion techniques like:

Encrypted communication to hide payloads.

Fragmented packets or tunneling to bypass detection.

Exploiting the limited visibility of low-interaction honeypots.

R.M.K GROUP OF INSTITUTIONS

3. **Data Collection Framework**

All observations from the firewall, IDS, and honeypots are aggregated into a centralized data collection system for analysis.

•Sources of Data:

Firewall logs.

IDS alerts and packet captures.

Honeypot host activity.

Network transaction records.

4. Data Capture Categories:

1.Network Transaction Recording

Tracks "who talks to whom" (IP addresses, ports, protocols).

Provides high-level visibility into attacker communication patterns.

2.Network Traffic Recording

Records raw packet data (payloads, headers).

Enables replay and deep packet inspection for malware/attack analysis.

3.Host Activity Recording

Monitors honeypot behavior (e.g., file system changes, command execution).

Provides insight into attacker techniques inside the honeypot.

4.IDS Alerts

Alerts generated by the IDS when malicious signatures or anomalies are detected.

Helps correlate suspicious traffic with honeypot activity.

R.M.K GROUP OF INSTITUTIONS

4. Case Study: Setup a honey pot and monitor the honey pot on network.

To deploy and monitor a honeypot using Cowrie, a popular SSH and Telnet honeypot. Honeypots are valuable tools for security research, as they can capture and analyze malicious activities.

Tools

Kali Linux: A Debian-derived Linux distribution designed for digital forensics and penetration testing.

Cowrie: A medium-interaction SSH and Telnet honeypot.

Docker: For setting up the Cowrie honeypot in a containerized environment

Installation

Docker

Install Docker on your Kali Linux machine:

sudo apt-get update

sudo apt-get install docker.io

sudo systemctl start docker

sudo systemctl enable docker

Pull te Crowrie Docker Image

sudo docker pull cowrie/cowrie

Run the Cowrie container:

sudo docker run -d -p 2222:2222 -p 2223:2223 --name cowrie cowrie/cowrie

Cowrie should now be running and listening on ports 2222 (SSH) and 2223 (Telnet).

R.M.K GROUP OF INSTITUTIONS

Task 1: Verify Honeypot Deployment

Step1: Open a terminal on your Kali Linux machine. Step2: Check if the Cowrie container is running:

sudo docker ps

Expected Output: The Cowrie container should be listed as running.

Task 2: Simulate an Attack

Step1: From your Kali Linux machine, attempt to connect to the honeypot using SSH:

ssh root@localhost -p 2222

Step2: Enter any password when prompted.

Expected Output: The honeypot should log the attempt and display a fake shell environment.

Task 3: Monitor Honeypot Logs

Step1: Access the logs of the Cowrie container:

sudo docker logs cowrie

Expected Output: The logs should show details of the SSH connection attempt, including the username, password, and commands entered.

R.M.K GROUP OF INSTITUTIONS

Task 4: Analyze Captured Data

Step1: Open another terminal on your Kali Linux machine. Step2: Access the Cowrie logs directory within the container:

sudo docker exec -it cowrie /bin/bash

cd /srv/cowrie/var/log/cowrie

Step3: Analyze the cowrie.json file for detailed logs of captured sessions:

cat cowrie.json | jq '.'

Expected Output: Detailed JSON log entries of the captured sessions, including connection attempts and command execution.

R.M.K GROUP OF INSTITUTIONS

10. ASSIGNMENT UNIT IV

SET 1

Demonstrate the use of Snort as a Network-based Intrusion Detection System (NIDS) in Kali Linux. How can Snort detect suspicious traffic such as port scans or denial-of-service attempts?

SET 2

How can brute-force attacks be simulated on a honeypot using tools like Hydra? What patterns in the honeypot logs reveal these brute-force attempts?

SET 3

Describe how honeypot logs can be integrated into a SIEM tool such as Splunk or ELK for centralized monitoring. How does visualization help in understanding attack patterns?

SET 4

How can custom Snort rules be written and implemented to detect port scanning attempts on Kali Linux? Explain with an example rule and the type of alerts it generates.

SET 5

Present a case study on setting up a honeypot in a Kali Linux environment. Explain the deployment process, monitoring of attacks, and analysis of the collected data for cyber threat detection.

R.M.K GROUP OF INSTITUTIONS

11. PART A Q & A (WITH K LEVEL AND CO) UNIT 4

1. **Define Intrusion Detection System (IDS).(K1,CO4)**

   An IDS is a security solution that monitors and analyzes activities on a network or host to detect suspicious or malicious actions. It generates alerts when unauthorized access or abnormal behavior is identified. IDS acts as an early warning system for potential security breaches.

2. **What is the difference between signature-based and anomaly-based detection?**

   (K2,CO4)

   Signature-based detection works by comparing traffic or activity with a database of known attack patterns. Anomaly-based detection, on the other hand, establishes a baseline of normal behavior and flags deviations. Signature-based is effective for known threats, while anomaly-based is useful against unknown or zero-day attacks

3. **Why is an Intrusion Detection and Prevention System (IDPS) important?(K2,CO4)**

   IDPS plays a crucial role in protecting organizations by continuously monitoring activities and detecting threats in real-time. Unlike IDS, it can also prevent malicious activities by blocking them. It improves system resilience, reduces downtime, and strengthens overall cybersecurity posture.

4. **Mention two limitations of traditional IDS.(K2,CO4)**

   Traditional IDS cannot prevent attacks; it only generates alerts. Another limitation is false positives, where normal activity is flagged as malicious, wasting administrator time. Additionally, IDS may struggle with encrypted traffic and high-speed networks.

5. **Differentiate between HIDS and NIDS.(K2,CO4)**

   A: Host-based IDS (HIDS) is installed on a specific machine and monitors log files, processes, and system integrity. Network-based IDS (NIDS) inspects network packets and analyzes communication between systems. HIDS is detailed at the host level, while NIDS covers broader network traffic.

R.M.K GROUP OF INSTITUTIONS

6. **Give one example of a network-based intrusion detection tool.(K2,CO4)**

Snort is a widely used open-source NIDS tool. It captures and analyzes packet traffic in real-time and applies rule-based patterns to detect intrusions. It is flexible and commonly used in research, enterprises, and academic experiments.

7. **Explain the role of an IPS.(K2,CO4)**

A: An Intrusion Prevention System (IPS) extends IDS capabilities by automatically taking action against threats. It blocks malicious packets, disconnects suspicious sessions, and prevents exploits from succeeding. IPS ensures active protection instead of just detection.

8. **What is the function of honeypots in cybersecurity?(K2,CO4)**

A: Honeypots are decoy systems designed to attract attackers. They allow security teams to observe attacker behavior, techniques, and tools without risking production systems. Honeypots also provide valuable data for developing better security measures.

9. **Differentiate between low-interaction and high-interaction honeypots.(K3,CO4)**

Low-interaction honeypots simulate only basic services (like SSH or FTP) and are safer but provide limited attacker data. High-interaction honeypots use real systems, giving attackers more freedom, which produces rich intelligence but carries higher risk.

10. **What are the advantages of using honeypots?(K2,CO4)**

A: Honeypots collect real-world attacker data, which helps improve defense strategies. They generate fewer false positives since any interaction is suspicious. They are cost-effective for research, provide early threat detection, and reveal emerging attack patterns.

11. **State one limitation of honeypots.(K2,CO4)**

A: Honeypots can only detect attacks directed at them and not those bypassing them. If attackers identify the honeypot, they may avoid or misuse it. Thus, honeypots work best as complementary tools rather than standalone defenses.

K-Level: K2

R.M.K GROUP OF INSTITUTIONS

12. **What is the use of Cowrie in honeypot experiments?(K1,CO4)**

Cowrie is an SSH/Telnet honeypot that logs attacker actions in detail. It captures brute-force attempts, executed commands, and files downloaded by attackers. This makes it an excellent tool for studying attacker techniques.

13**. Which type of data is collected by honeypots?(K2,CO4)**

A: Honeypots gather attacker IP addresses, login attempts, malware payloads, executed commands, and exploitation patterns. This data provides security researchers with actionable intelligence for threat prevention.

14. **What role do intrusion detection logs play in forensic investigation?(K3,CO4)**

IDS logs contain records of suspicious activities, timestamps, attacker details, and system responses. These logs serve as digital evidence in forensic investigations and help reconstruct attack scenarios.

R.M.K GROUP OF INSTITUTIONS

12. PART B Q s (WITH K LEVEL AND CO) UNIT III

1. Explain the need for Intrusion Detection Systems in cybersecurity. How do IDS and IPS complement each other in securing networks?(K3,CO4)
2. Compare and contrast Network-based IDS (NIDS) and Host-based IDS (HIDS) in terms of architecture, functionality, advantages, and limitations.(K4.CO5)
3. Discuss the challenges of intrusion detection in modern high-speed networks. Suggest techniques to overcome false positives and false negatives.(K4,CO4)
4. Describe the working of signature-based and anomaly-based intrusion detection with suitable examples. Which is more effective against zero-day attacks? Why?(K3,CO5)
5. Explain the role of honeypots in Intrusion Detection and Prevention. Differentiate between low-interaction and high-interaction honeypots with examples.(K3,CO4)
6. Case Study: Design and describe the setup of a honeypot in a networked environment using Kali Linux. How will you monitor and analyze attacker activities?(K4,CO4)
7. Illustrate the configuration and management of IDPS in an enterprise setting. Explain how logs, alerts, and reports help in proactive threat management.(K3,CO4)
8. Evaluate the effectiveness of honeypots in detecting modern cyber threats like ransomware and botnets. Discuss their advantages and limitations.(K4,CO4)

R.M.K GROUP OF INSTITUTIONS

13. Supportive online Certification courses

1. **UDEMY: SSL/TLS Fundamentals**

   https://www.udemy.com/course/ssl-tls-intro/

2. **COURSERA: Cryptography I**

   https://www.coursera.org/learn/crypto

3. **NPTEL : Cybersecurity and Privacy**

   https://onlinecourses.nptel.ac.in/noc25_cs116/preview

R.M.K GROUP OF INSTITUTIONS

14. Real time applications in day to day life and to Industry

Real-Time Application in Day-to-Day Life
Question:

Explain how Intrusion Detection Systems (IDS) and Honeypots are applied in real-world scenarios to enhance cybersecurity. Illustrate with examples from both daily user activities (such as banking, shopping, or home Wi-Fi) and industrial applications (such as enterprise networks, malware research, and insider threat detection)."

Expected Answer (Key Points):

IDS in Daily Life: Antivirus and firewall software on personal devices (e.g., Windows Defender) act as lightweight IDS, detecting suspicious activity on the host.

NIDS in Home/Enterprise Networks: Internet Service Providers (ISPs) and enterprise networks use Network-based IDS (NIDS) to monitor incoming/outgoing traffic and block malicious packets.

HIDS on Devices: Security tools like OSSEC or Tripwire act as Host-based IDS (HIDS) by monitoring changes in system files, logs, and unauthorized user access.

Honeypots for Research: Cybersecurity researchers deploy honeypots (like Cowrie or Dionaea) to capture attacker behavior, malware samples, and new hacking techniques.

Industry Applications: Enterprises use honeypots inside corporate networks to detect insider threats, phishing attempts, and botnet activity without risking real assets.

R.M.K GROUP OF INSTITUTIONS

15. ASSESSMENT SCHEDULE

Tentative schedule for the Assessment During 2024-2025 ODD semester

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	Unit Test 1			UNIT 1
2	IAT 1			UNIT 1 & 2
3	Unit Test 2			UNIT 3
4	IAT 2			UNIT 3 & 4
5	Revision 1			UNIT 5 , 1 & 2
6	Revision 2			UNIT 3 & 4
7	Model			ALL 5 UNITS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

16. PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXT BOOKS:

1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 2018.

REFERENCES:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Ravi Das and Greg Johnson, "Testing and Securing Web Applications", 2021.
3. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly Media, Inc, 2020.

R.M.K GROUP OF INSTITUTIONS

17 MINI PROJECTS SUGGESTIONS

Low-Interaction Honeypot for Web Attacks

Deploy Dionaea honeypot to capture malware samples.

Monitor HTTP requests (SQLi, XSS, brute force attempts).

Analyze collected malware or payloads in a sandbox.

IDS for IoT Devices

Simulate IoT devices (e.g., Raspberry Pi or virtual MQTT broker).

Configure Suricata IDS to detect unusual IoT traffic patterns.

Document findings and suggest improvements for IoT security.

Anomaly Detection using Machine Learning

Collect normal vs. attack traffic using Wireshark.

Train a simple ML model (Decision Tree / Random Forest) to classify malicious traffic.

Evaluate accuracy with test datasets.

Wireless Intrusion Detection (WIDS) with Kismet

Use Kismet or Aircrack-ng suite.

Detect rogue access points and deauthentication attacks on Wi-Fi.

Generate reports of wireless threats in a lab/home network.

Snort-based Network Intrusion Detection

Install Snort on Kali.

Configure rules to detect port scans, DoS attempts, and suspicious payloads.

Generate test traffic using Nmap and document alerts.

R.M.K GROUP OF INSTITUTIONS

18. GATE QUESTIONS

Q1. Which of the following best explains the need for Intrusion Detection Systems (IDS) in cybersecurity?

a) To encrypt sensitive data at rest

b) To detect unauthorized access or anomalies in system/network activities

c) To improve routing efficiency in a network

d) To provide authentication for user logins

Answer: b)

Q2. A Network-based Intrusion Detection System (NIDS) is primarily deployed:

a) On individual hosts to monitor log files

b) At network choke points to analyze traffic

c) To encrypt data for transmission

d) On firewalls to enforce access control policies

Answer: b)

Q3. Host-based IDS (HIDS) is more effective than NIDS in:

a) Detecting denial-of-service (DoS) attacks

b) Monitoring system-level file integrity and logs

c) Analyzing bandwidth utilization

d) Blocking suspicious IP addresses at the perimeter

Answer: b)

Q4. In the context of honeypots, which of the following is true?

a) Honeypots are used only for encrypting sensitive communication.

b) Honeypots provide real services to legitimate users.

c) Honeypots deliberately expose vulnerabilities to attract attackers.

d) Honeypots cannot be used with IDPS systems.

Answer: c)

R.M.K GROUP OF INSTITUTIONS

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.