NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech CSE
Course Code:	4CS209DE25
Course Title:	Intrusion Detection and Prevention Systems
Course Type:	Disciplinary Minor- Elective
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. outline various IDPS technologies, both signature-based and anomaly-based, including their strengths and weaknesses (BL2)
2. interpret the fundamental concepts and principles of cybersecurity, including the importance of intrusion detection and prevention (BL3)
3. examine various IDPS to assess its effectiveness in identifying and preventing intrusions (BL4)
4. evaluate different deployment strategies for IDPS in various network environments, including host-based, network-based, and hybrid solutions. (BL5)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to IDS and IPS:** Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anomaly detection – specification-based detection – hybrid detection, Types of IPS	07
Unit-II	**Classes of Attacks:** Network layer: scans, denial of service, penetration, Application layer: software exploits, code Injection, Human layer: identity theft, root access. Insider Threat issues – Taxonomy, Masquerade and Impersonation, Traitors, Decoys and Deception	09
Unit-III	**Signature-Based IDS/IPS, Anomaly-Based IDS/IPS:** Signature-based detection and prevention techniques, Snort and Suricata as examples, Signature rule creation Anomaly-based detection and prevention techniques, Machine learning and statistical approaches, Challenges and limitations	09
Unit-IV	**IDS/IPS Evasion Techniques:** Common evasion techniques, how to detect and prevent evasion, Testing IDS/IPS effectiveness, Theoretical Foundations of Detection Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering	12
Unit-V	IDS/IPS Integration with Security, Information, and Event Management (SIEM) The role of IDS/IPS in a SIEM ecosystem, Correlation, and incident response IDS/IPS Policy and Rule Management, Developing	08

and maintaining IDS/IPS policies, Rule management best practices, Rule optimization

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Richard Bejtlich, Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley Professional
2. Stephen Northcutt, Judy Novak, and Scott Winters, Network Intrusion Detection, Sams Publishing
3. Earl Carter, Intrusion Prevention Fundamentals, Cisco Press
4. Jack Koziol, Intrusion Detection with Snort, Sams Publishing
5. Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques, Springer

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Install and configure open-source IDS/IPS software like Snort or Suricata on a test network. Also, I will configure basic rule sets and test the system.	02
2	Capture and analyze network traffic using tools like Wireshark to understand normal network behavior.	02
3	Install Suricata, an alternative open-source IDS/IPS. Configure Suricata for intrusion detection and prevention. Test Suricata's rule sets and performance	02
4	Write custom Snort rules to detect specific network behaviors. Test the effectiveness of custom rules in detecting predefined attack patterns.	04
5	Use Snort to create and enforce firewall rules based on detected threats. Verify that the firewall rules effectively block malicious traffic.	04
6	Install and configure Bro/Zeek, an open-source network analysis framework. Set up anomaly detection rules in Bro/Zeek. Analyze the generated network logs to identify anomalies.	02
7	Install OSSEC, a host-based IDS/IPS. Configure OSSEC to monitor system logs and file integrity. Trigger and analyze alerts on the test system.	04
8	Deploy network-based IDS/IPS devices in the lab environment. Monitor network traffic and analyze alerts.	02
9	Set up a Security Information and Event Management (SIEM) system, such as ELK Stack. Integrate IDS/IPS alerts with the SIEM.	04
10	Explore the deployment of IDS/IPS solutions in a cloud environment. Configure cloud-based IDS/IPS to protect virtual networks.	04