Gyanmanjari Innovative University

Course Syllabus
Gyanmanjari Institute of Technology
Semester-7 (B.Tech)

Subject: Intrusion Detection and Prevention System– BETCE16407

Type of course: Professional Core

Prerequisite: Basic knowledge of computer networks, operating systems, cybersecurity concepts, and programming in Python, C, or Java is expected.

Rationale:

This course provides knowledge of detecting, analysing, and preventing cyber intrusions using network- and host-based security techniques. It prepares students for roles in cybersecurity, network security, and incident response.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
				Theory Marks		Practical Marks		CA	
CI	T	P	C	ESE	MSE	V	P	ALA	
4	0	2	5	60	30	10	20	30	150

Legends: CI-Classroom Instructions; T – Tutorial; P - Practical; C – Credit; ESE - End Semester Examination; MSE- Mid Semester Examination; V – Viva; CA - Continuous Assessment; ALA- Active Learning Activities.

Course Content:

Sr. No	Course Content	Hrs.	% Weightage
1	**Introduction to Intrusion Detection and Prevention Systems:** Fundamentals of information and network security, security threats and vulnerabilities, cyberattack lifecycle, concept and need of IDS and IPS, differences between IDS, IPS and firewall, IDS/IPS architecture and components, classification of intrusion detection systems, deployment modes and challenges.	12	20%
2	**Intrusion Detection Techniques:** Signature-based, anomaly-based, specification-based and hybrid detection, misuse detection, behaviour analysis, rule-based detection, statistical and machine-learning approaches, data collection and feature extraction, alert generation, false positives and false negatives, performance evaluation metrics.	12	20%
3	**Network-Based Intrusion Detection and Prevention:** Network traffic monitoring and packet analysis, Network-based IDS/IPS architecture, protocol analysis, detection of scanning, spoofing, DoS/DDoS, malware and web-based attacks, packet filtering, deep packet inspection, intrusion prevention techniques, introduction to Snort, Suricata and Zeek.	12	20%
4	**Host-Based and Distributed IDS/IPS:** Host-based IDS architecture, system logs, file integrity monitoring, process and user activity monitoring, rootkit and malware detection, application-based IDS, wireless IDS, distributed and cloud-based IDS, introduction to OSSEC/Wazuh, SIEM integration and centralized event monitoring.	12	20%
5	**IDS/IPS Deployment, Incident Response and Case Studies:** Planning and deployment of IDS/IPS, rule and policy configuration, alert analysis, log correlation, incident identification and response, system tuning and maintenance, ethical and privacy considerations, case studies of real-world cyberattacks, limitations, emerging trends and AI-based intrusion detection.	12	20%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Network Traffic Analysis and Intrusion Identification:** Each student will individually analyse a provided network traffic capture file using tools such as Wireshark or Zeek. Students will identify suspicious packets, unusual protocol behaviour, scanning attempts, authentication failures, or possible denial-of-service activity. The submission must include packet-level observations, identified indicators of compromise, screenshots, and a brief intrusion analysis report in PDF format on the GMIU Web Portal.	10
2	**IDS Rule Creation and Attack Detection Simulation:** Each student will configure an intrusion detection tool such as Snort or Suricata in an authorised laboratory environment. Students will create and test custom detection rules for activities such as port scanning, repeated login attempts, suspicious HTTP requests, or ICMP flooding. The submission must include rule configuration, testing procedure, generated alerts, screenshots, and an explanation of false positives and false negatives in PDF format on the GMIU Web Portal.	10
3	**Intrusion Detection and Incident Response Mini Project:** Students will work in groups to design and implement a basic IDS/IPS solution using tools such as Snort, Suricata, Wazuh, or OSSEC. The system should monitor network or host activities, detect selected security threats, generate alerts, and recommend suitable prevention or incident-response actions. The submission must include system architecture, tool configuration, detection results, alert analysis, response strategy, screenshots, and a project report in PDF format on the GMIU Web Portal.	10
	Total	30

Suggested Specification table with Marks (Theory): 60

Distribution of Theory Marks (Revised Bloom's Taxonomy)						
Level	**Remembrance (R)**	**Understanding (U)**	**Application (A)**	**Analyze (N)**	**Evaluate (E)**	**Create (C)**
Weightage %	10%	25%	25%	20%	15%	5%

Course Outcome:

After learning the course, the students should be able to:	
CO1	Explain the fundamentals, architecture, types, and components of Intrusion Detection and Prevention Systems.
CO2	Apply signature-based, anomaly-based, and hybrid techniques for intrusion detection.
CO3	Analyze network traffic and identify common cyberattacks using IDS/IPS tools.
CO4	Evaluate host-based, network-based, and distributed intrusion detection mechanisms.
CO5	Design and configure an IDS/IPS solution for threat detection and incident response.

List of Practical

Sr. No	Description	Unit No.	Hrs.
1	Install and configure a virtual cybersecurity laboratory using Linux and basic networking tools.	01	02
2	Capture and analyse network packets using Wireshark to identify normal and suspicious traffic.	01	02
3	Study signature-based and anomaly-based intrusion detection using sample network datasets.	02	02
4	Analyse port-scanning and service-enumeration activities in an authorised laboratory environment.	02	02
5	Evaluate IDS alerts and identify false positives and false negatives from provided security logs.	02	02

6	Install and configure Snort or Suricata for network traffic monitoring and intrusion detection.	03	04
7	Create and test custom IDS rules for ICMP traffic, port scanning, and suspicious HTTP requests.	03	04
8	Configure Wazuh or OSSEC for host-based monitoring, log analysis, and file-integrity checking.	04	04
9	Implement MQTT-based communication using broker-client model for efficient IoT data exchange.	05	04
10	Design and demonstrate a basic IDS/IPS solution for detecting threats and generating security alerts.	05	04
		Total	30

Instructional Method:

The course delivery method will depend upon the requirement of content and the needs of students. The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.
Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

Reference Books:

[1] Chris Sanders, Jason Smith – *Applied Network Security Monitoring: Collection, Detection, and Analysis* – Syngress/Elsevier, 1st Edition, 2013.
[2] Richard Bejtlich – *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* – No Starch Press, 1st Edition, 2013.
[3] Chris Fry, Martin Nystrom – *Security Monitoring* – O'Reilly Media, 1st Edition, 2009.
[4] Michael Collins – *Network Security Through Data Analysis* – O'Reilly Media, 2nd Edition, 2017.
[5] Kwangjo Kim, Muhamad Erza Aminanto, Harry Chandra Tanuwidjaja – *Network Intrusion Detection Using Deep Learning: A Feature Learning Approach* – Springer Singapore, 1st Edition, 2018.