SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)

SRM Nagar, Kattankulathur–603203

DEPARTMENT OF CYBERSECURITY

QUESTION BANK

V SEMESTER

1923503 - INTRUSION DETECTION SYSTEMS

Regulation– 2019

Academic Year 2022–2023(Odd Semester)

Prepared by

Ms. N.J.Subashini, A.P (Sl.G)/CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

S.R.M. Nagar, Kattankulathur - 603 203.

DEPARTMENT OF CYBER SECURITY

(ODD Semester 2022-2023)

SUBJECT : 1923503 – INTRUSION DETECTION SYSTEMS

SEM / YEAR : V SEMESTER/ THIRD YEAR

UNIT – I : INTRODUCTION
Network Attacks, Attack Taxonomies, Probes , IPSweep and PortSweep, NMap, MScan, SAINT, Satan, Privilege Escalation Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Worms Attacks , Routing Attacks

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	List the four improper conditions of computer attack	Remember	BTL1
2	Define VERDICT	Remember	BTL1
3	BGP attackers use 7 common mechanisms. List them	Remember	BTL1
4	Known attacks in Privilege Escalation Attacks can be generally divided into two categories. List them and explain	Remember	BTL1
5	What are the types of parameters passed between two system components to avoid improper validation	Remember	BTL1
6	What is worm attack	Remember	BTL1
7	In the fourth dimensions of Hansman's taxonomy, payloads are classified into five types. List them.	Remember	BTL1
8	Predict the two common protocols that are widely used in the implementation of Internet routers	Understand	BTL2
9	Give examples for Dictionary and FTP Write misconfiguration attacks.	Understand	BTL2
10	Summarize the main objectives of a BGP attack	Understand	BTL2
11	Describe improper randomness and improper deallocation	Understand	BTL2
12	Discuss ping of death	Understand	BTL2
13	Show the purpose of attack taxonomy	Apply	BTL3
14	Examine how a well-known buffer overflow attack was discovered in Microsoft Outlook and Outlook Express in 2000.	Apply	BTL3
15	In the second dimension Hansman's taxonomy, which are considered as attacker's targets?	Apply	BTL3
16	What are the different scanning tools that are used for network probing?	Apply	BTL3
17	Explain Netbait	Analyze	BTL4
18	Explain MITM attack	Analyze	BTL4

19	Explain OSPF attack	Analyze	BTL4
20	Explain BGP attack	Analyze	BTL4
21	Compared to VERDICT, Hansman's taxonomy is more complete and practical. Justify	Evaluate	BTL5
22	Compare IPSweep and PortSweep	Evaluate	BTL5
23	SAINT provides three optional modes of operation. List and explain them	Evaluate	BTL5
24	How the critical information system will be improperly exposed to the attack.	Create	BTL6
25	How MULTOPS are used in identifying attacks?	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	a. Payloads are classified into five types in the fourth dimensions of Hansman's taxonomy. Explain each. (7) b. List any 3 real time examples for DoS and DDoS Attacks (6)	Remember	BTL1
2	In detail, explain the WEBSOS ARCHITECTURE with a neat diagram. (13)	Remember	BTL1
3	a. State the main objective of attacker in BGP attack(8) b. Explain Bishop's vulnerability taxonomy(5)	Remember	BTL1
4	a. What are software vulnerabilities? Give example of different types of vulnerabilities (7) b. Many models and techniques are used to prevent software vulnerabilities. Explain (6)	Remember	BTL1
5	Explain how software vulnerabilities can be prevented. (13)	Remember	BTL1
6	a. Discuss in detail about the characteristics of some well-known worm attacks appeared recently with a large-scale outbreak in Internet and affecting a large number of systems and services.(6) b. Explain the different SPF insiders attacks for evaluating a real-time protocol-based intrusion detection system (7)	Understand	BTL2
7	Explain well-known privilege escalation attacks with example. (13)	Understand	BTL2
8	Discuss in detail about the classification of IDS. (13)	Understand	BTL2
9	What is DDos? Explain in detail. (13)	Understand	BTL2
10	Illustrate in detail about the different scanning tools that are used for network probing? (13)	Apply	BTL3
11	Demonstrate how Routing attacks exploit flaws and vulnerabilities in the design and implementation of routers. (13)	Apply	BTL3
12	With a diagram explain how the effectiveness of attacks depends on the Autonomous System (AS) topology and on the location of the compromised router relative to the victim network. (13)	Apply	BTL3
13	Explain the various detection approached of DoS and DDoS Attacks. (13)	Analyze	BTL4

14	a. In Hansman's taxonomy, the first dimension attacks have been classified into ten 10 categories. Point out them. (10) b. How Intrusion Prevention System (IPS) are classified (3)	Analyze	BTL4
15	a. Privilege escalation attacks have two categories of known attach? Explain (4) b. How Prevention and Response for DoS and DDoS Attacks take place? (10)	Analyze	BTL4
16	Summarize the four dimensions of Hansman's taxonomy? Explain any two in detail. (13)	Evaluate	BTL5
17	Explain in detail about the Detection Methodologies for DDoS Attacks and solution for Trace back with a neat diagram. (13)	Evaluate	BTL5
18	a. How traditional epidemic models are applied to model the spread of the Internet worms and to analyze their magnitude by some researchers. (6) b. How worm attacks are detected and monitored? (7)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Illustrate how IDS are classified into 5 types. (15)	Evaluate	BTL5
2	Explain in detail about Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks. (15)	Evaluate	BTL5
3	Summarize the different approaches to Intrusion Detection and Prevention. (15)	Evaluate	BTL5
4	Describe in detail about the four dimensions of Hansman's taxonomy. (15)	Create	BTL6
5	With some examples explain the different types of attacks of well-known privilege escalation attacks. (15)	Create	BTL6

UNIT – II : DETECTION APPROACHES

Detection Approaches, Misuse Detection, Pattern Matching, Rule–based Techniques, State– based Techniques, Techniques based on Data Mining, Anomaly Detection, Advanced Statistical Models, Rule based Techniques, Biological Models , Learning Models, Specification–based Detection, Hybrid Detection

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Name and explain three different intrusion detection approach	Remember	BTL1
2	Define IDIOT	Remember	BTL1
3	What are the members of STAT family?	Remember	BTL1
4	Write about hierarchical hybrid intelligent system model	Remember	BTL1
5	What is Rule-Based technique? Give example	Remember	BTL1
6	Summarize the strength and the weaknesses of host based Ids approaches	Remember	BTL1
7	Define hybrid intrusion detection system	Remember	BTL1
8	Summarize supervised and unsupervised learning techniques	Understand	BTL2
9	Differentiate supervised and unsupervised learning techniques	Understand	BTL2

10	NADIR collects audit information from three different kinds of service nodes. State and discuss them	Understand	BTL2
11	Give example for Graphic Turing Tests	Understand	BTL2
12	Three types of algorithms are particularly useful for mining audit data. Summarize them	Understand	BTL2
13	Denning detection framework, which is based on basic statistical analysis, consists of eight components. Classify them	Apply	BTL3
14	Illustrate the advantages of pattern matching in misuse detection approach	Apply	BTL3
15	Show the limitations of Rule-based Technique in misuse detection	Apply	BTL3
16	Hyperview is an early attempt for intrusion detection using neural network, which consists of two components. Classify them and Explain	Apply	BTL3
17	Nine distinct pattern recognition and machine learning algorithms were tested on the KDD dataset. Classify them	Analyze	BTL4
18	Explain EMERALD	Analyze	BTL4
19	State the advantages and disadvantages of anomaly detection	Analyze	BTL4
20	The structure of the rules in the P-BEST rule base includes two layers. Explain	Analyze	BTL4
21	Which system was designed and implemented for the detection of intrusions in a multi-user Air Force computer system. Explain	Evaluate	BTL5
22	Wisdom & Sensor is a unique approach to anomaly detection. Justify	Evaluate	BTL5
23	Which is considered as the first intrusion detection system using network traffic directly as the primary source of data?	Evaluate	BTL5
24	Draw the misuse detection model	Create	BTL6
25	Illustrates an example of MIDAS rule	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	Describe in detail about Specification-based and hybrid Detection. (13)	Remember	BTL1
2	Describe about y mean clustering algorithm. (13)	Remember	BTL1
3	Identify how State-based techniques detect known intrusions by using expressions of the system state and state transitions. (13)	Remember	BTL1
4	a. What is anomaly detection used for?(7) b. List the various detection method of IDS:(6)	Remember	BTL1
5	Write in detail about the Data types in Anomaly Detection. (13)	Remember	BTL1
6	Discuss in detail about Advanced Statistical Models in Anomaly detection. (13)	Understand	BTL2
7	Predict how Rule-based expert system is one of the techniques used for misuse detection. (13)	Understand	BTL2
8	Explain the system architecture of Hybrid Multi-level Intrusion Detection System. (13)	Understand	BTL2

9	Differentiate the Rule-based techniques in Anomaly Detection and Misuse Detection. (13)	Understand	BTL2
10	Demonstrate how anomaly detection models were implemented using rule-based techniques. (13)	Apply	BTL3
11	Illustrate Supervised Anomaly Detection in detail. (13)	Apply	BTL3
12	a. Illustrates a simple example of CPA with a diagram(7) b. Classify the various detection method of IDS (6)	Apply	BTL3
13	Explain Unsupervised Anomaly Detection in detail. (13)	Analyze	BTL4
14	Point out any three distinct pattern recognition and machine learning algorithms which were tested on the KDD dataset and elaborate them in detail. (13)	Analyze	BTL4
15	How GASSATA is considered as one of the earliest attempts for using genetic algorithm (GA) for intrusion detection. Give example and Explain. (13)	Analyze	BTL4
16	Explain k mean clustering algorithm. (13)	Evaluate	BTL5
17	Explain how misuse or signature detection system works with a diagram. (13)	Evaluate	BTL5
18	With a diagram explain the misuse detection model and any two of its classes of technique. (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Explain in detail about anomaly-detection. (15)	Evaluate	BTL5
2	Summarize in detail about the learning techniques which have been widely used in anomaly detection. (15)	Evaluate	BTL5
4	Classify and describe in detail about the different types of Rule-Based technique in misuse-detection. (15)	Evaluate	BTL5
3	Demonstrate the technique used to detect known intrusions by using expressions of the system state and state transitions.	Create	BTL6
5	With a diagram explain the misuse detection model and its four classes of technique. (15)	Create	BTL6

UNIT – III : DATA COLLECTION AND THEORETICAL FOUNDATION

Data Collection, Data Collection for Host–Based IDSs, Audit Logs, System Call Sequences and Data Collection for Network–Based IDSs, Theoretical Foundation of Detection, Taxonomy of Anomaly Detection Systems, Fuzzy Logic, Architecture and Implementation, Centralized, Distributed, Intelligent Agents, Mobile Agents and Cooperative Intrusion Detection

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Define Audit logs.	Remember	BTL1
2	List the features used by Kruegel et al. for characterizing each application	Remember	BTL1
3	Even though system-calls prove to be a good information source for intrusion detection at the application layer, they still face several limitations. Identify them	Remember	BTL1

4	Traditional approaches to intrusion detection are centralized and have two major limitations. What are they?	Remember	BTL1
5	Write the Pros and cons of Signature-based intrusion detection methodologies	Remember	BTL1
6	List and describe the three types of output to report the anomalies.	Remember	BTL1
7	List the three categories of audit data created by the Solaris OS	Remember	BTL1
8	Discuss about fuzzy membership function	Understand	BTL2
9	Describe ScanAID	Understand	BTL2
10	Give the three parts of Hummingbird system and explain	Understand	BTL2
11	What are the four categories of multi-agent IDS	Understand	BTL2
12	Which IDS is based on a fully distributed, multi-agent framework? What are its 4 major components	Understand	BTL2
13	Demonstrate the use of *Syslogd* and *auditdin Solaris OS*	Apply	BTL3
14	There are some basic principles of information sharing among networks which are helpful to identify and counter large-scale Internet attacks. Classify any 4 principles.	Apply	BTL3
15	Using Sensor (S-box), Manager (MS-box) and Console Software draw Overall Design of the FAST System	Apply	BTL3
16	Show how the IDA system focuses on detecting intrusions efficiently, instead of detecting precisely all intrusions	Apply	BTL3
17	Which have been proved to be an effective information source in host-based intrusion detection. Explain it	Analyze	BTL4
18	Analze the advantages and disadvantages of single packet/flow capture engine	Analyze	BTL4
19	Classify the main objective of Hummingbird system	Analyze	BTL4
20	Classify the advantages of Hummingbird System	Analyze	BTL4
21	System Health and Intrusion Monitoring architecture includes the host SHIM sensors and a centralized SHIM manager. Assess the use of sensor and manager and explain.	Evaluate	BTL5
22	There are three operating modes defined for anomaly detection techniques. Describe them	Evaluate	BTL5
23	Summarize the basic idea behind using system calls for intrusion detection	Evaluate	BTL5
24	How the anomaly detection methods are categorized based on the method they use to report the anomalies	Create	BTL6
25	Design the table for the patterns extracted from a SC sequence using a sliding window of 3 calls	Create	BTL6
PART-B (13 Marks)			
Q.No	**Question**	**Competence**	**Level**
1	Describe in detail about Data Collection for Host-Based IDSs. (13)	Remember	BTL1
2	a. Explain centralized IDS architecture with a neat diagram(6) b. Explain distributed IDS architecture with a neat diagram(7)	Remember	BTL1

3	List the Pros and cons of Signature-based (knowledge-based), Anomaly-based (behavior-based), and Stateful protocol analysis (specification-based) intrusion detection methodologies. (13)	Remember	BTL1
4	Identify the two phases of modeling the normal network traffic. Explain with a diagram. (13)	Remember	BTL1
5	Explain in detail with a diagram about the implementation architecture for the FAST system. (13)	Remember	BTL1
6	Predict the two types of mobile-agent based IDSs. Discuss them in detail. (13)	Understand	BTL2
7	Discuss in detail about Data Collection for Network-Based IDSs	Understand	BTL2
8	Write the comparisons between different IDS technology types such as HIDS, NIDS and WIDS. (13)	Understand	BTL2
9	a. Describe in detail about the three operating modes that are defined for anomaly detection techniques.(7) b. In addition to the types of training sets, anomaly detection methods can be categorized based on the method they use to report the anomalies. Summarize the three types of output to report the anomalies.(6)	Understand	BTL2
10	Demonstrate how the mobile information-gathering agent in IDA collects information related to MLSIs from a target system. (13)	Apply	BTL3
11	a. Demonstrate how External and internal sensors for direct data collection have different strengths and weaknesses, and can be used together in an intrusion detection system. Explain (8) b. Point out the advantages and disadvantages of External and internal sensors(5)	Apply	BTL3
12	How the limitation created by centralized intrusion system is overcome by the Intelligent agent? Explain. (13)	Apply	BTL3
13	Why System Call sequences have proved to be an effective information source in host-based intrusion detection. Explain	Analyze	BTL4
14	a. There are some basic principles of information sharing among networks which are helpful to identify and counter large-scale Internet attacks. Point out all the principles.(10) b. Explain Adaptive Hierarchical Agent-based Intrusion Detection System. (3)	Analyze	BTL4
15	a. Explain in detail about Autonomous Agents for Intrusion Detection (AAFID)(6) b. Explain in detail about Hummingbird System(7)	Analyze	BTL4
16	Summarize in detail about Taxonomy of Anomaly Detection Systems. (13)	Evaluate	BTL5
17	Explain VM architecture with a neat diagram. (13)	Evaluate	BTL5
18	With a neat diagram explain Fuzzy Adaptive Survivability Tools. (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Explain in detail about Data Collection for Network-Based IDSs. (15)	Evaluate	BTL5

2	How Fuzzy logic is used in IDS. Explain. (15)	Evaluate	BTL5
3	Summarize distributed IDS architecture with a neat diagram. (15)	Evaluate	BTL5
4	Discuss in detail about Cooperative Intrusion Detection. (15)	Create	BTL6
5	Demonstrate in detail about Data Collection for Host-Based IDSs. (15)	Create	BTL6

UNIT – IV : ALERT MANAGEMENT AND CORRELATION

Detection Approaches, Misuse Detection, Pattern Matching, Rule–based Techniques, State– based Techniques, Techniques based on Data Mining, Anomaly Detection, Advanced Statistical Models, Rule based Techniques, Biological Models , Learning Models, Specification–based Detection, Hybrid Detection

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Define Belief Function	Remember	BTL1
2	Describe Data fusion?	Remember	BTL1
3	What is interest-based cooperation and communication	Remember	BTL1
4	List any four components of Alert correlation.	Remember	BTL1
5	Identify the two modes in which ALAC can be operated	Remember	BTL1
6	Quote the XML representation for IDMEF messages	Remember	BTL1
7	What is directed and propagated interest	Remember	BTL1
8	State the Rule of Combination in D-S theory	Understand	BTL2
9	How Token Bucker Filter is used to tackle the alert flood problem	Understand	BTL2
10	Consider the buffer overflow attack against the sadmind remote administration tool, *SadmindBufferOverflow =({VictimIP, VictimPort}, {ExistHost(VictimIP) & VulnerableSadmind(VictimIP)}, {GainRootAccess(VictimIP)}).* Explain the different attributes in it	Understand	BTL2
11	Give two examples for D-S theory data fusion in intrusion detection	Understand	BTL2
12	What is Alert correlation?	Understand	BTL2
13	In addition to the aggregation, alert compression is another simple technique for dealing with duplicate alerts. Explain the technique	Apply	BTL3
14	Illustrate the purpose of using alert aggregation	Apply	BTL3
15	For obtaining the overall similarities between new alert and meta alert, four metrics are considered. What are they?	Apply	BTL3
16	Alerts are considered to be aggregated in terms of their attributes. List the different attributes included.	Apply	BTL3
17	D-S theory can be considered as extension of Bayesian inference. How?	Analyze	BTL4
18	In alert correlation process, for the sake of generalization, it is divided into three stages based on the general data process procedure. Classify and explain them	Analyze	BTL4
19	How hierarchical propagation of interests are divided? Explain	Analyze	BTL4

20	Analyze what are the three components are there in alert the alert correlation framework	Analyze	BTL4
21	Explain Generalized Alarm in alarms clustering technique	Evaluate	BTL5
22	Explain Generalized Hierarchies in alarms clustering technique	Evaluate	BTL5
23	What are the syntax and semantics used by STATL	Evaluate	BTL5
24	Write the formula for computing the overall similarities between new and meta alert	Create	BTL6
25	Create the XML code for IDMEF alert	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	a. List and explain the different components for ID agent and ID correlator. (7) b. In the first experimental validation of correlation systems, there are three primary dimensions of high level reasoning that enable correlators to recognize attack (6)	Remember	BTL1
2	a. Explain the mathematical framework of D-S theory.(7) b. An Alert message is composed of nine aggregate classes. List them and explain briefly (6)	Remember	BTL1
3	Explain in detail about the Alert Correlation Based on Known Scenarios approach. (13)	Remember	BTL1
4	Name the correlation approach which is based on the assumption that most alerts are not isolated, but related to different stages of attacks. Describe in detail. (13)	Remember	BTL1
5	Discuss in detail about Intention or plan Recognition. (13)	Remember	BTL1
6	a. Provide the three required abstraction to capture the common characteristics between different compositions of frequent patterns, and explain how the patterns should be generalized(6) b. Explain the terms Alarm, Generalized Attribute Value, Generalized Alarm and Generalization Hierarchies(7)	Understand	BTL2
7	a. Write the mathematical framework of D-S theory and explain (10) b. Summarize the 3 stages of alert correlation (3)	Understand	BTL2
8	Discuss how alert correlation approach correlates alerts based on the similarities of some selected features, such as source IP addresses, destination IP addresses, and port numbers. (13)	Understand	BTL2
9	List the different Correlation technique and discuss them in detail. (13)	Understand	BTL2
10	Explain Data fusion in detail. (13)	Apply	BTL3
11	Which standard format for intrusion alerts was drafted by the IETF Intrusion Detection Working Group (IDWG). Demonstrate with a model diagram(13)	Apply	BTL3
12	Identifying the false positives and dealing or filtering them out or using them for further analysis, can significantly reduce the number of alerts that need to be further processed. Illustrate how these false alerts are reduced. (13)	Apply	BTL3

13	a. In M-Correlator model, how the final assessment of a security incident is calculated? (6) b. How efficient the plan recognition system in IDS will be able to handle in different situation? (7)	Analyze	BTL4
14	Explain post processor technique in alert correlation. (13)	Analyze	BTL4
15	Several principles of information sharing have been identified in the development of a framework for cooperation among domains. Classify them. (13)	Analyze	BTL4
16	Consider the scenario for ftp-write attack, in which an attacker creates a bogus *.rhost* file in any user's home directory using the ftp service. Having the file, the attacker is able to open a remote session using *rlogin* service. How this scenario can be described using STATL specification? (13)	Evaluate	BTL5
17	Explain in detail about M-Correlator model. (13)	Evaluate	BTL5
18	Design a diagram and explain in detail about Date Normalization. (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Explain Alert Correlation in detail. (15)	Evaluate	BTL5
2	Discuss about Cooperative Intrusion Detection. (15)	Evaluate	BTL5
3	Data reduction is a critical process to reduce the number of alerts without losing important information. Justify. (15)	Evaluate	BTL5
4	Demonstrate in detail how the Preprocess techniques are used to normalize the alert data, eliminate redundancy and tackle the false positive problem. (15)	Create	BTL6
5	Point out the different Correlation technique. Explain them in detail. (15)	Create	BTL6

UNIT – V : EVALUATION CRITERIA

Evaluation Criteria, Accuracy, False Positive and Negative, Confusion Matrix, Precision, Recall, and F–Measure, ROC Curves, The Base–Rate Fallacy, Performance, Completeness, Timely Response, Intrusion Tolerance and Attack Resistance, Redundant and Fault Tolerance Design and Test, Evaluation and Data Sets

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	What is Base-Rate Fallacy	Remember	BTL1
2	List and describe the two rules in NIDS	Remember	BTL1
3	Distinguish between Signature-based vs. Anomaly-Based	Remember	BTL1
4	What are the types of IDS?	Remember	BTL1
5	List and explain the four categories of Pattern Recognition approach.	Remember	BTL1
6	What do ids detect?	Remember	BTL1
7	Tabulate the difference between Header-Based vs. Payload-Based	Remember	BTL1
8	Give example for each two-class nature of intrusion detection	Understand	BTL2
9	Summarize the different cost factors of intrusion detection and response systems	Understand	BTL2

10	IDES uses P-BEST to describe its rule. Explain the two rules	Understand	BTL2
11	What are attacks detected by NIDS	Understand	BTL2
12	Difference Between Firewall And Intrusion Detection System	Understand	BTL2
13	Which metric measures the missing part from the Precision? Demonstrate	Apply	BTL3
14	Which uses the properties of both precision and Recall? Explain	Apply	BTL3
15	Specify Some of the Leading Intrusion Detection Systems (IDS) Products?	Apply	BTL3
16	There are three levels of connection features. Classify them.	Apply	BTL3
17	Why the intrusion monitoring and analysis moved from the target system to a separate system?	Analyze	BTL4
18	What will happen if the IDS does not launch or launch a response for an incorrect detection?	Analyze	BTL4
19	To enhance the security what are the functionalities NIDS can perform.	Analyze	BTL4
20	REMUS prototype design is based on the analysis of critical system calls. What is System call? How the system calls have been partitioned in level of threat?	Analyze	BTL4
21	The Confusion Matrix is a ranking method applied to any kind of classification problem. Justify	Evaluate	BTL5
22	Cost-sensitivity also be considered in the process of developing and evaluating IDSs. How?	Evaluate	BTL5
23	Explain the analysis originates from the signal detection theory.	Evaluate	BTL5
24	Design the ROC curve for different classifiers	Create	BTL6
25	Design a diagram to represent how the Macro-components are positioned within the security system framework	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	Describe how network traffic can be effectively represented through the definition of an appropriate set of traffic features. (13)	Remember	BTL1
2	Explain reference model for a real-time network Intrusion Detection System (IDS) based on Pattern Recognition techniques. (13)	Remember	BTL1
3	Explain in detail intrinsic features, traffic features and content features. (13)	Remember	BTL1
4	In order to solve the issue related to data set building, two main approaches are possible. Explain both approaches in detail. (13)	Remember	BTL1
5	State the privacy issues in IDS. (13)	Remember	BTL1
6	Write a short note of a. Precision, Recall, and F-Measure (6) b. False Positive and Negative(7)	Understand	BTL2
7	Summarize a distributed version of the proposed IDS. (13)	Understand	BTL2
8	Discuss in detail about Real time intrusion detection system. (13)	Understand	BTL2
9	Illustrate with a diagram Active Security System architecture. (13)	Understand	BTL2

10	Classify and explain each ASP protocol messages. (13)	Apply	BTL3
11	Show how the ASSYST router infrastructure has been used for traffic classification and intrusion reaction. (13)	Apply	BTL3
12	Snort library of functions are used to manage the Splay Trees. What is splay Trees? Explain the different trees implemented from it. (13)	Apply	BTL3
13	The system response is the most important step when combating an attack. How? Explain with example. (13)	Analyze	BTL4
14	a. In order to understand the usage of the ROC curves in detecting the accuracy of a classifier, several points on the ROC space must be described. Explain (6) b. Explain how the IDS performance is evaluated(7)	Analyze	BTL4
15	Analyze what are the measurements that can be made on IDSs that relate to detection accuracy. (13)	Analyze	BTL4
16	With real time example explain Base-Rate Fallacy. (13)	Evaluate	BTL5
17	Explain how the efficiency of IDS is improved by using Distributed IDS with a diagram. (13)	Evaluate	BTL5
18	Draw and explain the generic IDS architecture, which consists of four components and its transformation using DFFA structure. (13)	Create	BTL6
	PART-C (`15 Marks)		
Q.No	**Question**	**Competence**	**Level**
1	Accuracy is a statement of how correct an IDS works, measuring the percentage of detection and failure. Analyze. (15)	Evaluate	BTL5
2	Although there is not any standard test framework capable of comprehensive evaluation of proposed prototypes, there are several data sets that have been used throughout the recent years. Explain any five of them. (15)	Evaluate	BTL5
3	Explain in detail about Intrusion Tolerance and Attack Resistance	Evaluate	BTL5
4	With a detailed block diagram explain in detail about the evaluation test bed. (15)	Create	BTL6
5	Demonstrate how the Background traffic is necessary to determine the false alarm rates of intrusion detection systems. (15)	Create	BTL6