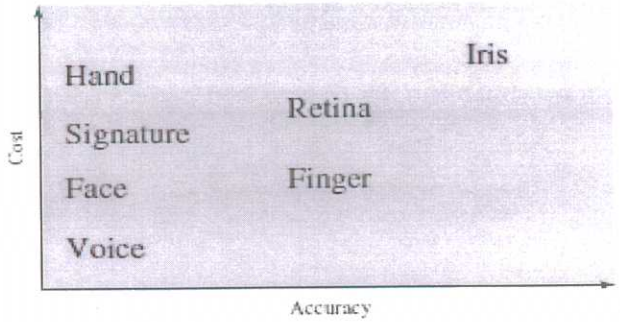
SCHEME OF VALUATION

(Scoring Indicators)

Revision: 2015	Course Code: 5136			
Course Title : INFORMATION SECURITY				
Qst. No.	**Scoring Indicator**	**Split up score**	**Sub Total**	**Total**
	PART A	½ marks		
1.	Confidentiality, Integrity, Availability, Authenticity, Accountability	each		2
2.	1) It prevents duplicate passwords from password file 2) It increases the difficulty of offline dictionary attacks 3) It is almost impossible to find out whether a person has used same password in multiple systems (Any two enough)	1 for each		2
3.	• Controls access based on the identity of user and the access rules or authorizations allowed for that user • Policy is called discretionary because the user might have access rights (discretionary power) that permit him to enable others to access some resource.	2		2
4	• Virus , Logic Bombs, Backdoors	2		2
5	• An attack against availability of resources or service • It is an action that prevents or impairs the authorized use of networks, system or applications by exhausting resources such as CPU, memory, bandwidth, disk space etc.	2		2

	PART – B			
1.	• Draw diagram (***diagram-1***) • Explain the terms : ○ Assets (Hardware , Software , Data & networks) ○ Vulnerabilities (corrupted , leaky , unavailable) ○ Threat - a potential security harm to asset , exploits vulnerability ○ Attack – threat action (passive or active) ○ Threat agent – is the attacker	Diagram : 2 Explanation 4		6

	○ Countermeasure – prevent, detect, respond & recovery ○ Vulnerability & threat decides the level of risk to the system			
2.	• Draw Diagram (***diagram -2***) • Public-key certificate is one of the solutions to the forgery of public-key. • A certificate consists of: a) A public key b) User ID of the owner of public key c) Information about a third party Certificate Authority (CA) and period of validity. • The whole block containing the above three information is digitally signed by the Certificate Authority. The digital signature is created using CA's private key. • A user can present his/her public key to the CA in secure manner and obtain the certificate. The user can then publish the certificate. Anyone who need the user's public key can obtain the certificate and verify its validity by means of attached signature.	Diagram : 2 Explanation : 4		6
3.	**Static Features** 1. **Facial Characteristics :**The common approach is to define characteristics based on relative location and shape of key facial features, such as eyes, eyebrows, nose , lips and chin shape 2. **Fingerprints** : A fingerprint is a pattern of ridges and furrows on the surface of the fingertip. Fingerprints are believed to be unique across the entire human population 3. **Hand geometry :**Hand geometry systems identify features of the hand including shape, lengths and widths of fingers 4) **Retinal Pattern :** The pattern formed by veins beneath the retinal surface is unique and therefore suitable for identification 5) **Iris :** The detailed structure of iris is another unique physical characteristics **Dynamic Features** 6) **Signature :** Each individual has unique way of handwriting which is reflected especially in signature . So signatures can be used for identification • Disadvantage is , multiple signature samples from a single individual will not be identical which complicates the task of developing computer signature to match with future samples.	5 + 1		6

	7. **Voice :** Voice samples are better than signature ***Cost versus Accuracy of Various Biometric Characteristics***  Figure 3.5 **Cost versus Accuracy of Various Biometric Characteristics in User Authentication Schemes** (Any 5 + Comparison graph)			
4.	• SNORT is an open source, highly configurable, portable , light weight, host-based or network-based IDS • ***Diagram - 3*** • Explain briefly the four logical components - Packet Decoder , Detection engine , Logger , Alerter • SNORT NIDS can be configured with passive sensor or inline sensor . Inline sensor can provide the functionality of intrusion prevention also.	Diagram : 2 Explanation: 4		6

5.	• Need for constructing attack network :
	  ○ A S/w with capability to communicate with attacker, conceal its existence , triggering mechanism, launch attack to target
	  ○ Vulnerable systems
	• Identify vulnerable systems by Scanning or finger printing
	• Common scanning strategies – Random, Hit-list , Topological , Local-subnet
	•A BOT once installed in a system, that will repeat the scanning process until a large distributed network is created known as BOTNET
		4 * 1.5		6

6.	**Capabilities of a firewall** 1. A firewall defines a single choke point in a network that simplifies security management. 2. A firewall provides a location for monitoring security-related events. 3. A firewall is a convenient platform for several Internet functions that are not security related. (eg : NAT) 4. A firewall can act as the platform for IPSec to implement virtual	3 + 3		6

	private networks. **Limitations of Firewall** 1) The firewall cannot protect against attacks that bypass the firewall 2) The firewall may not protect fully against internal threats, such as a disgruntled (unhappy) employee or an employee who unintentionally cooperates with an external attacker. 3) An improperly secured wireless LAN may be accessed from outside the organization 4) A laptop, PDA, or portable storage device may be used and infected outside the corporate network and then attached and used internally. (Any 3 capabilities & limitations enough)			
7.	**Concept** :- It is a type of denial of service (DoS) attack that use packets with **forged source addresses**. **Action of attacker** • If an attacker gets sufficient privileges to access the network handling code on a computer system, it is easy to create packets with a forged source address. • The attacker normally generates ***large volumes of packets***. • Source addresses randomly selected might be of real systems or unreachable addresses. ***How the action becomes an attack?*** • Packets with spoofed source address will be sent over the same path towards the target system that ***will cause congestion in lower capacity link***. The response packets would be scattered across the Internet to all the various forged source addresses. **Advantage to attacker** : It is difficult to identify the attacking system due to the use of forged source addresses in packets. **To detect the attack**, the flow of packets of some specific form through the routers along the path from the source to the target system must be identified. **To counter the attack**, advanced filter configurations must be imposed on routers.	6 x 1		6

III a)	PART C - Unit I Draw the 3 block diagrams - ***Diagram 4*** a) **Encrypt the message digest using symmetric encryption**	Diagram – 4.5		9

	The message digest can be encrypted and if the key is shared by only the sender and the receiver, then authenticity is assured b) **Encrypt the message digest using public key encryption** Public key approach has **two** advantages: 1. It provides message authentication as well as digital signature 2. It does not require distribution of keys to communicating parties. • Both symmetric and public key encryption approach has an advantage that they do not encrypt the entire message. So less computation is required. **3. Only using secret values without encryption** • Here, there is no encryption at all. This technique is called keyed hash MAC. • Here both sender A and receiver B share a common key K, which is used for generating hash code. • When A sends a message M to B, the hash code or message digest is calculated as: MDM = H (K || M || K) Then it transmits [M || MDM] • Since B has the secret key K, it will compute H (K || M || K) and verify MDM As long as the secret key remains secret, an attacker cannot generate a false message.	Explanation – 4.5		
b)	Resources are Hardware , Software, Data & Communication networks * Theft of CD, DVD etc can lead to loss of **confidentiality**.	4 x 1.5		6

	AVAILABILITY	CONFIDENTIALITY	INTEGRITY
HARDWARE	Equipment is stolen or disabled thus deny service.	-	-
SOFTWARE	Deletion of programs	An unauthorized copy of software is made.	A working program is modified. The program either fails or do some wrong task.
DATA	File deletion deny access to users.	Unauthorized read of data. Analysis of statistical data may reveal underlying data.	Modify existing files. Fabricate new files.
COMMUNICATION LINES	Deletion or destruction of messages network or lines are made unavailable.	Reading of messages observing traffic patterns.	Modification, delaying, reordering or duplication of message. Fabrication of false messages.

IV	PART C - Unit I	2 + 7		9

a)	• The managers responsible for security in an organization need a systematic approach to assess the security needs, to evaluate and choose security products and policies. Security architecture for OSI defines such a systematic approach. • OSI security architecture is useful to managers to organize the task of providing security. • It is an international standard followed by communication and computer vendors while making their products and services. Security mechanisms are mainly classified as **two**: **1) Specific security mechanisms :** These are implemented in a specific protocol layer such as TCP or an application layer protocol. **2) Pervasive security mechanisms :** These are services which are not specific to any protocol layer or security service. <u>List of specific security mechanism</u> 1. Encipherment 2. Digital signature 3. Access control: 4. Data integrity 5. Authentication exchange 6. Traffic padding 7. Routing control 8. Notarization <u>List of pervasive security mechanisms</u> 1. Trusted Functionality 2. Security label 3. Event detection. 4. Security audit trial 5. Security recovery (Explain each briefly)			
b)	• Draw the block diagram ***Diagram - 5*** • Public Key encryption or asymmetric key encryption need a pair of keys. • Each party has a pair of keys (one is public key and can be collected by anybody and the other is private key which is known only by the owner)	Diagram – 2 + Explanation – 4		6

	• No need to exchange a secret key between communicating parties. • Whatever data is encrypted using a public key can be decrypted only by its pair private key and vice versa. • **To achieve confidentiality, the sender encrypts the message using receiver's public key** so that only the receiver will be able to decrypt and see the message using his/her private key • Diagram shows the ingredients and the working			

V a)	PART C - Unit II 1. Concept of UNIX file system (inode, hierarchical structure) 2. User ID & Group ID to individual users 3. 12 Permission bits to each object o Read, Write , Execute permission for owner, group & others (9 – bits) o **Set UserID & Set GroupID** bits gives effective User ID & Group ID permission to files while running. Set Group ID bit for folders determine the default group of files created inside that folder. o Use of **Sticky Bit** for files & folders 4. Super User Concept 5. Extended Access List (with Mask) used with latest UNIX versions • Draw ***diagrams – 6*** (minimal & extended access control lists)	Diagram : 2 Explanation : 7		9
b)	➢ **Something the individual knows** A password, PIN (Personal Identification Number), answers to a prearranged set of questions ➢ **Something an individual possesses** Electronic keycards, smart cards, physical keys. These things are known as tokens. ➢ **Something the individual is (static biometrics)** fingerprint, retina, face ➢ **Something the individual does (dynamic biometrics)** Voice pattern, handwriting characteristics. Typing rhythm	4 * 1.5		6

	All of these methods, if properly implemented and used , can provide secure user authentication However each method has its own issues. An attacker may be able to guess or steal password. An attacker may be able to steal or forge token. With respect to biometric authentication, the major problems are false positives, false negatives, user acceptance, cost, and convenience.			

VI a)	PART C - Unit II Remote user authentication faces the security threats such as: – An eavesdropper can capture a password – An adversary can replay an observed authentication sequence The countermeasure for the threats to remote user authentication is the use of some form of **challenge-response** protocol	4 + 4		8

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow [r, E()]$	r, random number $E()$, function
$B' \rightarrow BT'$ biometric D' biometric device r', return of r	$E(r', D', BT') \rightarrow$	$E^{-1}E(r', P', BT') = (r', P', BT')$
	← yes/no	if $r' = r$ and $D' = D$ and $BT' = BT(U)$ then yes else no

(c) Protocol for static biometric

- In this challenge-response protocol,
- User sends his/her ID to the remote host
- Host generates and transmits a challenge with a random number **r** called **nonce** and an encryption identifier **E()**
- At the user end, the client system will have a biometric device which provides the user's biometric
- The client system **responds** to the host with **E(r', D',BT')** where **r' = r** and **D'** is the ID of biometric device and **BT'** is the biometric template of the user.
- The host decrypts the incoming message to recover the three parameters and compares these to locally stored values

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{r, x, E()\}$	r, random number x, random sequence challenge E(), function
B', $x' \rightarrow BS'(x')$ r', return of r	$E(r', BS'(x')) \rightarrow$	$E^{-1}E(r', BS'(x')) = (r', BS'(x'))$ extract B' from $BS'(x')$
	$\leftarrow$ yes/no	if $r' = r$ and $x' = x$ and $B' = B(U)$ then yes else no

(d) Protocol for dynamic biometric

In this challenge-response protocol,

- User sends his/her **ID** to the remote host
- Host generates and transmits a challenge with a random number r called **nonce,** a random sequence and an encryption identifier **E()**
- Random sequence is a sequence of numbers, characters or words
- Human user at the client side must then vocalize (speaker verification), type (keyboard dynamic verification), or write (handwriting verification) the sequence to generate a biometric signal **BS'(x').**
- The client encrypts the **BS'(x')** and the random number and send to the host. Host generates a comparison based on the incoming biometric signal **BS'(x')**, the stored template **BT(U)** for this user and the original signal **x** and the random number

b)	1. Reliable input: 2. Support for fine and coarse specifications 3. Least privilege 4. Separation of duty 5. Open and closed policies: 6. Policy combinations and conflict resolution 7. Administrative policies 8. Dual Control (Explain any 7 points)	7 x 1		7

VII a)	PART C - Unit III • A standard format is required to facilitate the	Need : 2		8

	development of distributed IDSs which may require interoperability with heterogeneous systems or environments • Draw diagram of model (***Diagram -7***) • Explain the elements – Data source , Sensor, Analyzer, Administrator, Manager , Operator	Diagram :2 Key Elements :4		
b)	1) Multiplatform 2) Multiexploit 3) Ultrafast spreading 4) Polymorphic 5) Metamorphic 6) Transport Vehicle 7) Zero-day Exploit (explain briefly about each types)	7 *1 =1		7

VIII a)	PART C - Unit III Two general approaches **Anomaly detection : -** 1) Collect data related to legitimate user for a period of time. Then statistical test are applied to observed behaviour to determine the anomalies and detect intrusion , if any. 2) Two approaches for anomaly detection: profile-based , threshold detection 3) Anomaly detection is suitable for masqueraders (outside intruders) . May not be suitable with misfeasors (insiders) **Signature Detection :** 1) Set of rules or attack patterns are used to decide that the a given behaviour is that of an intruder 2) Most suitable for misfeasors 3) Two approaches : **Rule-based anomaly detection** (Rules are generated automatically by analysing the historic audit records) and **Rule-based penetration identification** (Rules are developed by analysing attack tools, scripts collected from internet etc.) Briefly explain about significance of audit records (Various metrics: counter, gauge, interval-timer, resource	3+3+3		9

	utilization. Statistical test approaches: mean, standard deviation, multivariate, Markov process etc.)			
b)	○ A rootkit is a set of malicious programs that maintain root access to a system ○ Alters the host's standard operations in a malicious and stealthy way ○ Changes programs and files ○ Monitor processes ○ Send and receive network traffic ○ Get backdoor access on demand ○ Changes system to hide its existence	6 x 1		6

IX	PART C - Unit IV			
a)	**Distributed denial-of-service attacks(DDoS)** • DDoS is **an indirect** type of DoS that uses **multiple systems** to generate attack. • These systems were typically compromised user workstations or PCs known as **Zombies.** • The attacker installs their own programs on these systems by exploiting any flaw in the operating system or other applications. Once suitable "**backdoor**" programs were installed on these systems, they were entirely under the attacker's control • Large collections of **Zombies** under the control of one attacker can be created, collectively forming a "**botnet**". • A control hierarchy is used as shown in figure. (***Diagram -8***) • A small number of systems act as **handlers** controlling a much larger number of **agent** systems. • The attacker can send a single command to a handler, which then automatically forwards it to all the agents under its control. • Once the agent software is uploaded to a newly compromised system, it can contact one or more handlers to automatically notify them of its availability. By this means, the attacker can	Diagram : 2 Explanation : 6		8

	automatically grow suitable **"botnets"**. • Instead of using spoofed source address, **DDoS relies on a large number of compromised systems and layered command architecture to hide the path** back to the attacker. • **Handler programs are usually simple command-line programs or IRC (Internet Relay Chat)** which is used to communicate with agents. • Many of the **attack tools use cryptographic mechanism** to authenticate agents to the handlers in order to prevent analysis of command traffic. • **Defense** : Prevent your systems from being compromised (Follow good system security practices, update OS, applications etc. regularly).			
b)	• A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. • Typically, the bastion host serves as a platform for an application-level or circuit-level gateway. **Common characteristics of a bastion host:** 1. The bastion host hardware executes a secure version of its operating system, making it a trusted system. 2. Only essential proxy services such as Telnet, DNS, FTP, SMTP etc. are installed in Bastian Host 3. Each proxy is configured to support only a subset of the application's command set. 4. Each proxy is configured to allow access only to specific host systems. 5. Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. 6. Each proxy is independent of other proxies on the bastion host, and can be uninstalled without affecting the operation of the other proxy applications. 7. A proxy generally performs no disk access other than to read its initial configuration file. This read-only configuration makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files.	1+6		7

	8. Each proxy runs as a non-privileged user in a private and secured directory on bastion host. (Any 6 characteristics + definition)			

	PART C - Unit IV			
X a)	**Packet Filtering Firewall**: • Applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet . Packet filter firewall works in the network layer. • The firewall is typically configured to filter packets going in both directions (from and to the internal network). • Filtering rules are based on information contained in a network packet: source IP address, • destination IP address, source and destination transport-level address (port number), IP • protocol field, and interface (on firewall packet came from or is destined for). • One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast. • Disadvantage is it may face certain attacks such as IP address spoofing , source rooting attacks, tiny fragment attacks etc. **Stateful Inspection Firewalls**: • A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context • A Stateful Inspection Firewalls reviews the same packet information but also records information about TCP connections so that further inbound traffic will be allowed only for the established connections. • May also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. • Stateful Inspection Firewall operates at the transport	Diagrams : 2 Explanation : 3+3		2 + 6

	layer ***Diagram - 9***			
b)	Reflection & Amplification attacks : Amplification attack is one type of reflection attack • Both are indirect DoS attacks using multiple intermediate systems • Intermediate systems are normal systems like network servers in both cases. • In both attacks, the attacker will create malicious packets with spoofed source address of target and will send those packets to selected vulnerable intermediate systems. • Packets will be created with suitable protocols so that it will generate responses directed to the spoofed target. When it happens from multiple systems, it will become an attack on the target. • In particular, amplification attacks follows **two** strategies to amplify the attack volume. ○ Attacker sends the malicious packet to the broadcast address of intermediate network so that the reflection will be generated from all systems in the network ○ Amplification can also be achieved by selecting DNS servers as intermediary by exploiting its behavior of generating largest size responses to the requests coming to it. Diagrams showing particular scenarios (***Diagram -10***)	Diagram : 2 Explanation : 5		7