



S J P N Trust's

Hirasugar Institute of Technology, Nidasoshi.*Inculcating Values, Promoting Prosperity*Approved by AICTE, Recognized by Govt. of Karnataka and Affiliated to VTU Belagavi.
Accredited at "A" Grade by NAAC & Recognized Under Section 2(f) of UGC Act, 1956.

ECE Dept.

Exam.

Internal Assessment

Even Sem(2018-19)

SECOND INTERNAL ASSESSMENT

Sem: VIII

Date: 12/04/2019

Sub: Network and Cyber Security

Time: 11AM-12Noon

Sub. Code: 15EC835

Max. Marks: 25

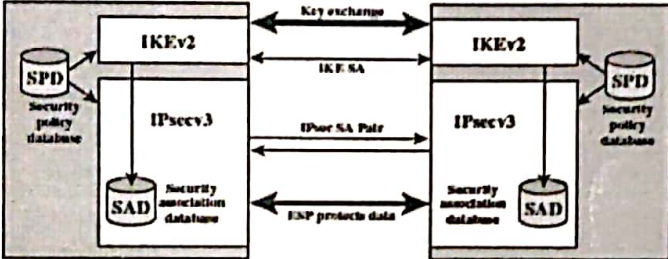
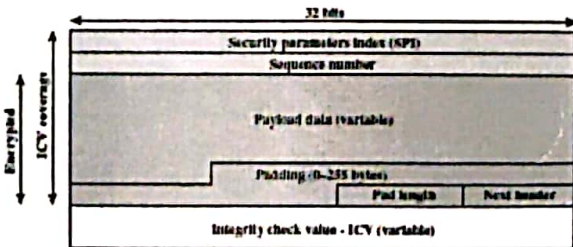
Note: Answer two full questions, draw sketches wherever necessary.

Q. No	Description of Question	Marks	CO	RBT LEVEL
1	a Explain IP Security Policy architecture along with Security Associations (SA).	6	C411E.3	L2
	b Explain Encapsulating Security Payload (ESP) Format.	7	C411E.3	L2
OR				
2	a Explain Internet Key Exchange (IKE) formats.	6	C411E.3	L2
	b Explain basic combinations of Security Associations.	7	C411E.3	L2
3	a Explain typical hardware setup sequences for a desktop pedestal.	6	C411E.5	L2
	b Explain Zachman framework for enterprise architecture.	6	C411E.5	L2
OR				
4	a Explain managing administrations and root accounts.	6	C411E.5	L2
	b Explain mini patterns for problem solving meetings.	6	C411E.5	L2

Prof. B. P. Khot
Course CoordinatorProf. N. M. Patel
Module CoordinatorDr. V. G. Kasabegoudar
HOD



IA - II SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
1	a	<p>Explain IP Security Policy architecture along with Security Associations (SA).</p> <ul style="list-style-type: none"> Fundamental to the operation of IP Security (IPsec) is the concept of a security policy applied to each IP packet that transits from a source to a destination. IPsec policy is determined primarily by the interaction of two databases, the security association database (SAD) and the security policy database (SPD). A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA).  <ul style="list-style-type: none"> A security association is uniquely identified by three parameters. <ol style="list-style-type: none"> Security Parameters Index (SPI): A 32-bit unsigned integer assigned to this SA and having some local significance only. IP Destination Address: This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router. Security Protocol Identifier: This field from the outer IP header indicates whether the association is an AH or ESP security association. 	6	C411E.3	L2	
	1	b	<p>Explain Encapsulating Security Payload (ESP) Format.</p> <ul style="list-style-type: none"> ESP can be used to provide confidentiality, data origin authentication, connectionless, integrity, an anti-replay service and traffic flow confidentiality.  <p>(a) Top-level format of an ESP Packet</p>		7	C411E.3

B. B. B.
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD



IA - II SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
		<p>(b) Substructure of payload data</p> <ol style="list-style-type: none"> Security Parameters Index (32 bits): Identifies a security association. Sequence Number (32 bits): A monotonically increasing counter value Payload Data (variable): This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption. Padding (0-255 bytes) Pad Length (8 bits): Indicates the number of pad bytes immediately preceding this field. Next Header (8 bits): Identifies the type of data contained in the payload data. Field by identifying the first header in that payload Integrity Check Value (variable): A variable-length field Two additional fields may be present in the payload Initialization value (IV): or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP. If tunnel mode is being used, then the IPsec implementation may add traffic flow confidentiality (TFC) padding after the Payload Data and before the Padding field, as explained subsequently. 	2			
2	a	<p>Explain Internet Key Exchange (IKE) formats. An IKE message consists of an IKE header followed by one or more payloads. All of this is carried in a transport protocol. The specification dictates that implementations must support the use of UDP for the transport protocol.</p> <p>(a) IKE header</p> <p>(b) Generic Payload Header</p> <p>IKE Header Format</p>	6	C411E.3	L2	
			3			

Belagavi
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD



IA - II SCHEME OF EVALUATION

Sem :VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
2	b	<p>Figure shows the header format for an IKE message. It consists of the following fields.</p> <ul style="list-style-type: none"> Initiator SPI: A value chosen by the initiator to identify a unique IKE security association (SA). Responder SPI : A value chosen by the responder to identify a unique IKE SA. Next Payload (8 bits): Indicates the type of the first payload in the message; payloads are discussed in the next subsection. Major Version (4 bits): Indicates major version of IKE in use. Minor Version (4 bits): Indicates minor version in use. Exchange Type (8 bits): Indicates the type of exchange Flags (8 bits): Indicates specific options set for this IKE exchange. Message ID (32 bits): Used to control retransmission of lost packets and matching of requests and responses. Length (32 bits): Length of total message (header plus all payloads) 	3			
		<p>Explain basic combinations of Security Associations. The IPsec Architecture document lists four examples of combinations of Security Associations(SA) As that must be supported by compliant IPsecuity hosts (e.g., workstation, server) or security gateways (e.g., firewall, router). These are illustrated in Figure.</p> <p>Figure: Basic Combinations of Security Associations Case 1. All security is provided between end systems that implement IPsec. For any two end systems to communicate via an SA, they must share the appropriate secret keys. Among the possible combinations are a. AH in transport mode b. ESP in transport mode c. ESP followed by AH in transport mode d. Any one of a, b, or c inside an AH or ESP in tunnel mode</p>	7	C411E.3	L2	

Padote
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD



S J P N Trust's

Hirasugar Institute of Technology, Nidasoshi.

*Inculcating Values, Promoting Prosperity*Approved by AICTE, Recognized by Govt. of Karnataka and Affiliated to VTU Belagavi.
Accredited at "A" Grade by NAAC & Recognized Under Section 2(f) of UGC Act, 1956

ECE Dept.

Exam.

Scheme of Evaluation

Even Sem(2018-19)

Page. No. 4 / 6

IA - II SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
3	a	<p>Case 2. Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. The security architecture document specifies that only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required, because the IPsec services apply to the entire inner packet.</p> <p>Case 3. This builds on case 2 by adding end-to-end security. The same combinations discussed for cases 1 and 2 are allowed here. The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic between end systems.</p> <p>Case 4. This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall. As in case 1, one or two SAs may be used between the remote host and the local host.</p> <p>Explain typical hardware setup sequences for a desktop pedestal. Hardware setup sequence for a desktop pedestal includes the following:</p> <ul style="list-style-type: none"> Position the components on top of the desk. Optionally, if the system has a separate floor pedestal then it is placed on the desk along with the UPS, with the backside and connector ports facing the installer. Connect the monitor pigtail (power cable) and display cable and secure the thumbscrews. Feed the monitor, mouse, and keyboard cables down through a desktop opening, or around the back/side. Connect the network, monitor, mouse, and display cables to the pedestal. For a new UPS, you may need to connect the battery and charge. Connect the pigtail to the pedestal and then connect it to the UPS. Connect the UPS to the electrical outlet. Turn on the UPS. Double-check all cable connections. Always verify your work. Make no assumptions. Turn on the computer; verify that the monitor displays the boot sequence on the screen. If an operating system is installed, continue booting to check keyboard, mouse, and network functionality. Alternatively you can test the system using bootable CD/DVD test tools, such as BackTrack, Caine, or Helix. 	4			
	b	<p>Explain Zachman framework for enterprise architecture.</p> <ul style="list-style-type: none"> An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. The intent of an enterprise architecture is to determine how an organization can most effectively achieve its current and future objectives. The Zachman Framework is a widely used intellectual standard used to analyze and represent enterprise architectures. 	6	C411E.5	L2	

T. Belagavi
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD



IA - II SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description		Marks	CO's	RBT LEVEL
		<ul style="list-style-type: none"> It is an intellectual tool for describing enterprises. The Zachman Framework (see Figure) slices and dices complexity into rows and columns. The columns are the six basic questions you could ask about any subject. These interrogatives include: What? How? Where? Who? When? Why?. <p align="center">The Zachman Framework for Enterprise Architecture <i>The Enterprise Ontology</i></p>		3		
4	a	<p align="center">Zachman framework for enterprise architecture</p> <p>Explain managing administrations and root accounts. Some key best practices for managing privileged accounts include:</p> <ul style="list-style-type: none"> All users, including network administrators, should normally use unprivileged, nonadministrative accounts. Administrative operations should be effectively separated from other user activities. These policies are essential for network security for the following reasons: <ol style="list-style-type: none"> A network administrator, logged in as root superuser, visits a drive-by malware website; a rootkit is installed unknowingly. Now the attackers have administrative privileges on the network. Logged in with a privileged account, a user receives an unexpected but authentic-looking e-mail and opens its attachment, which installs a rootkit. A rootkit is malicious software that takes complete control of an account for a remote attacker. By compromising a privileged account, the entire system all its accounts, computing power, and data are compromised. 		6	C411E.5	L2
				3		

Staff-In-Charge

Module Coordinator

HOD



S J P N Trust's

Hirasugar Institute of Technology, Nidasoshi.

*Inculcating Values, Promoting Prosperity*Approved by AICTE, Recognized by Govt. of Karnataka and Affiliated to VTU Belagavi.
Accredited at "A" Grade by NAAC & Recognized Under Section 2(f) of UGC Act, 1956

ECE Dept.

Exam.

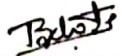
Scheme of Evaluation

Even Sem(2018-19)

Page. No. 6 / 6

IA - II SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 12/04/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
4	b	<p>Windows To create a privileged shell, choose Start → All Programs → Accessories and then right-click Cmd (command shell) and select Run as Administrator.</p> <p>VMware •ESXi (VM infrastructure os) is a sparse operating system, whose entire purpose is to administer virtual machines. It allows for all network administrators to use privileged accounts on this operating system.</p> <p>Linux and Unix The administrative account in Linux and Unix is username root. •From a nonroot account, Linux users can switch to root with the superuser command, su -, which challenges you for the root password.</p>	3			
		<p>Explain mini patterns for problem solving meetings. There are six mini patterns for problem solving meetings:</p> <ol style="list-style-type: none"> 1. Breakouts : Meetings are least productive when only one person talks and everyone else does nothing but listen and take notes. In general, people's creativity is inhibited in groups larger than five. The facilitator can ask that the group form small discussions to address a particular question, and then have them report back their conclusions subgroup by subgroup. Another approach is to quickly generate a list of topics or concerns and then have each breakout take one problem to solve as a subgroup before debriefing the general session. 2. Flipcharts: flipcharts give a group unlimited space for creativity. When a page of a flipchart is filled, it is moved and taped to a nearby wall. Flipcharts are also highly portable, unlike whiteboards. 3. Time Management : If you plan an agenda, plan the time of each meeting topic, and stick to it. Time consciousness keeps people focused on problem solving. 4. Ground Rules: Have some ground rules for each meeting so that distractions are minimized, and the group doesn't waste time. 5. Idea Parking Lot: Post a separate flipchart to capture ideas that are outside the meeting's purpose. Revisit these ideas at the end of the meeting and decide as a group how they should be addressed. 6. Other Problem-Solving Catalogs: General problem solving and business meeting facilitation are similar disciplines, and they share common catalogs of techniques. 	6	C411E.5	L2	


Staff-In-Charge


Module Coordinator


HOD