



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)

FIRST INTERNAL ASSESSMENT

Sem: VIII

Date: 15/03/2019

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 Secure Sockets Layer (SSL) with session state and connection state.	6	C411E.1	L2
	b Explain Transport Layer Security (TLS).	7	C411E.1	L2
OR				
2	a Explain Handshake Protocol.	6	C411E.1	L2
	b Explain Secure Shell (SSH) Protocol.	7	C411E.1	L2
3	a Explain antipattern concept and forces in antipatterns.	6	C411E.4	L2
	b Explain signature-based malware detection versus polymorphic threats.	6	C411E.4	L2
OR				
4	a Explain full cyber antipattern template.	6	C411E.4	L2
	b Explain refactored solution using reputational, behavioral, and entropy based malware detection.	6	C411E.4	L2


Prof. B. P. Khot
Course Coordinator


Prof. N. M. Patel
Module Coordinator


Dr. V. G. Kasabegoudar
HOD

**IA - I SCHEME OF EVALUATION**

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019																	
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL																
1	a	<p>Explain Secure Sockets Layer (SSL) with session state and connection state.</p> <ul style="list-style-type: none"> Most widely used security service Subsequently Became Internet Standard Known As TLS (Transport Layer Security) Originally Developed By Netscape SSL is a general purpose service provider, implemented as a set of protocol that relay/depend on TCP. Uses TCP to provide a Reliable End-to-end Service <div style="text-align: center;"> <table border="1"> <tr> <td>SSL Handshake Protocol</td> <td>SSL Change Cipher Spec Protocol</td> <td>SSL Alert Protocol</td> <td>HTTP</td> </tr> <tr> <td colspan="4">SSL Record Protocol</td> </tr> <tr> <td colspan="4">TCP</td> </tr> <tr> <td colspan="4">IP</td> </tr> </table> <p>Figure 1. SSL Architecture</p> <p>Two important SSL concept are</p> <ol style="list-style-type: none"> SSL Session SSL Connection <p>A session state is defined by the following parameters</p> <ul style="list-style-type: none"> Session identifier Peer certificate Compression method Cipher spec Master secret Is resumable <p>A connection state is defined by the following parameters</p> <ul style="list-style-type: none"> Server and client random Server write MAC secret Client write MAC secret Server write key Client write key Initialization vectors Sequence numbers </div>	SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol	HTTP	SSL Record Protocol				TCP				IP				6	C411E.1	L2
SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol	HTTP																		
SSL Record Protocol																					
TCP																					
IP																					
1	b	<p>Explain Transport Layer Security (TLS).</p> <p>Transport Layer Security</p> <ul style="list-style-type: none"> TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. The current draft version of TLS is very similar to SSLv3. Transport Layer Security (TLS) is a protocol that provides authentication, privacy, and data integrity between two communicating computer applications. 	7	C411E.1	L2																

Behot
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. 2 / 6

IA - I SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
2	a	Version Number The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version values. For the current draft of TLS, the Major Version is 3 and the Minor Version is 1.	2			
		Message Authentication Code There are two differences between the SSLv3 and TLS MAC schemes: the actual algorithm and the scope of the MAC calculation. TLS makes use of the HMAC algorithm defined in RFC 2104. HMAC is defined as follows: $HMACK_K(M) = H[(K+ XOR opad) H[(K+ XOR ipad) M]]$ Where H = embedded hash function (for TLS, either MD5 or SHA-1) M = message input to HMAC K+ = secret key padded with zeros on the left so that the result is equal to the block length of the hash code (for MD5 and SHA-1, block length = 512 bits) Ipad = 00110110 (36 in hexadecimal) repeated 64 times (512 bits) opad = 01011100 (5C in hexadecimal) repeated 64 times (512 bits)	3			
		Explain Handshake Protocol. <ul style="list-style-type: none"> • Most complex part of SSL • It allows server & client to: <ul style="list-style-type: none"> ○ authenticate each other ○ To negotiate encryption & MAC algorithms ○ to negotiate cryptographic keys to be used <ol style="list-style-type: none"> 1. Phase- 1 Establish Security Capabilities <ul style="list-style-type: none"> • The client initiates a logical connection "client_hello" • Parameters: version, random, session ID, cipher suite, compression Methods • Details of cipher suite: key exchange method • "server hello" 2. Phase -2 Server Authentication and Key Exchange <ul style="list-style-type: none"> • Server sends its certificate: one or chain of X.509 certificates; • Server sends a server_key_exchange message; • Server sends a certificate_request message • Certificate type and a list of CAs • Server sends a server_hello_done message 3. Phase -3 Client Authentication and Key Exchange <ul style="list-style-type: none"> • Client first verify server's certificate and parameters Received. If all good → • If server requests a certificate, client sends a certificate message • Client sends a client_key_exchange message • Client sends a certificate_verify message 	6	C411E.1	L2	


Staff-In-Charge


Module Coordinator


HOD



IA - I SCHEME OF EVALUATION

Sem :VIII	Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL
		<p>4. Phase -4 Finish</p> <ul style="list-style-type: none"> Client sends a change_cipher_spec message Client sends a finished message Verify the key exchange and authentication process were successful Server sends a change_cipher_spec message Server send a finished message <p>--- handshake is complete ---</p> <p>Note: Shaded transfers are optional or situation-dependent messages that are not always sent.</p>	1		
2	b	<p>Explain Secure Shell (SSH) Protocol.</p> <ul style="list-style-type: none"> SSH is a protocol for secure network communication Simple and inexpensive to implement. SSH provides secure remote access between client/server and can be used for file transfer and e-mail. Transmission can be compressed. SSH is organized as three protocols, run on top of TCP <ol style="list-style-type: none"> Transport layer Protocol User authentication Protocol Connection Protocol Functions of SSH protocol stack <ol style="list-style-type: none"> Transport layer protocol: Provides server authentication, data confidentiality and integrity User authentication protocol: Authenticates the user to the server Connection protocol: Multiplex multiple logic communication channels over a single SSH connection 	6	C411E.1	L2
			2		
			2		

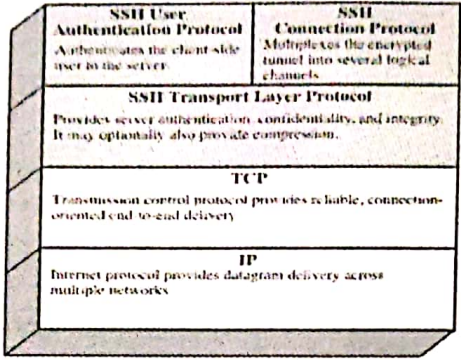
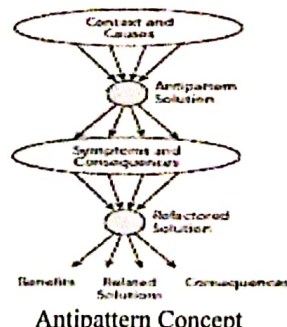
Belat
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD



IA - I SCHEME OF EVALUATION

Sem :VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
3	a	 <p>Figure: SSH protocol</p>	2			
		<p>Explain antipattern concept and forces in antipatterns.</p> <p>Antipatterns Concept:</p> <ol style="list-style-type: none"> Design forces are the competing concerns, priorities, and technical factors that influence the choice of solutions. In antipatterns, there are two solutions: The antipattern solution and the refactored solution. An antipattern solution represents a commonplace dysfunctional situation or configuration. Every solution or design choice yields benefits and consequences(result). The refactored solution results from a reconsideration of the design forces and the selection of a more effective solution. 	6	C411E.4	L2	
		 <p>Antipattern Concept</p> <p>Forces in Cyber Antipatterns</p> <ul style="list-style-type: none"> The major types of forces in antipatterns include primal, horizontal, and vertical forces. <ol style="list-style-type: none"> Primal design forces present in almost every design decision. Horizontal forces are forces that can apply in all domains. Vertical forces are domain or system specific design forces. The primal design forces in the cybersecurity domain include: <ol style="list-style-type: none"> Management of functionality Management of confidentiality Management of integrity Management of availability 	2			

Tadot
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD

**IA - I SCHEME OF EVALUATION**

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
3	b	<p>Explain signature-based malware detection versus polymorphic threats.</p> <ul style="list-style-type: none"> The conventional wisdom (belief) is that all systems with up-to-date antivirus signatures will be safe. However, many popular antivirus solutions are nearly obsolete, with many missing the majority of new malware. Malicious signature growth is exploding from 5 new ones per day in 2000 to 1,500 per day in 2007 and more than 15,000 per day in 2009, according to Symantec report. Each security industry vendor has its own sensor network for gathering and monitoring malware. Kaspersky Labs has seen flat growth in malware signatures since 2008, while other vendors imply exponential growth. In Polymorphic malware Threats: Changing a string in the file is sufficient to trigger a false negative in file. Some polymorphic techniques include varying character encodings, encryption, and random values in the files. 	6	C411E.4	L2	
4	a	<p>Explain full cyber antipattern template.</p> <p>The full cyber antipattern template has two main parts: a header and a body. The heading fields in the full cyber antipattern template are</p> <ul style="list-style-type: none"> Antipattern Name: The name is a unique noun phrase of antipattern. Also Known As: Many antipatterns are known by various names across different organizations. Refactored Solution Names: Unbalanced Primal Forces: This field lists the primal design forces that are poorly resolved by this antipattern Template. Anecdotal Evidence: These evidences characterize this antipattern. <p>The body fields in the full cyber antipattern template are</p> <ul style="list-style-type: none"> Antipattern Solution: This field defines the antipattern solution through diagrams, explanations and examples, and discussions of design forces. Causes, Symptoms, and Consequences: The intent is to make it easier to recognize the threat and understand how and why its replacement is necessary. Known Exceptions: If there are some situations where the antipattern solution might be desirable, this section identifies them. Refactored Solution and Examples: The refactored solution is proposed as an alternative to the antipattern solution. Related Solutions: If there are other potential solutions to the antipattern, they are identified in this section. 	6	C411E.4	L2	
4	a	<p>Explain refactored solution using reputational, behavioral and entropy based malware detection.</p> <ul style="list-style-type: none"> The technique, called reputation-based signatures, is able to identify 240 million new malware signatures by comparing binaries across millions of systems for anomalous variations. Ex: Symantec 	6	C411E.4	L2	

Belost
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. 6 / 6

IA - I SCHEME OF EVALUATION

Sem : VIII		Subject : Network and Cyber Security	Sub Code : 15EC835	Date : 15/03/2019		
Q. No.	Bit	Description	Marks	CO's	RBT LEVEL	
		<ul style="list-style-type: none">• FireEye has created a behavioral intrusion detection system (IDS) that uses elements of honeypots and forensics to automatically identify malicious content as it flows across corporate networks.• An emerging field of research called entropy-based malware detection looks for mathematical similarity to known malware signatures. Hash functions that are used by most antivirus programs detect subtle differences between a file and its known hash. Minor changes to a file, such as modification of strings or encodings can cause a hash match to fail.	2 2			

Palak
Staff-In-Charge

[Signature]
Module Coordinator

[Signature]
HOD