

**NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY, THENI.**

<b>Course/Branch</b> : B.E /ECE	<b>Year / Semester</b> :IV/VII	Format No.	NAC/TLP-07a.13
<b>Subject Code</b> :EC 8702	<b>Subject Name</b> :Adhoc Wireless Sensor Networks	Rev. No.	02
<b>Unit No</b> :5	<b>Unit Name</b> : Sensor Network Platforms And Tools	Date	30.09.2020

**OBJECTIVE TYPE QUESTION BANK**

<b>S. No.</b>	<b>Objective Questions (MCQ /True or False / Fill up with Choices )</b>	<b>BTL</b>
1	Automatic protection switching in linear network is defined at the _____ <b>a) line layer</b> b) section layer c) photonic layer d) path layer	L2
2	A unidirectional path switching ring is a network with _____ a) one ring <b>b) two rings</b> c) three rings d) four rings	L2
3	What is SDH? a) sdh is similar standard to SONET developed by ITU-T b) synchronous digital hierarchy <b>c) sdh stands for synchronous digital hierarchy and is a similar standard to SONET developed by ITU-T</b> d) none of the mentioned	L4
4	Real-time transport protocol (RTP) is mostly used in _____ a) streaming media b) video teleconference c) television services <b>d) all of the mentioned</b>	L5
5	RTP is used to _____ <b>a) carry the media stream</b> b) monitor transmission statistics of streams c) monitor quality of service of streams d) secure the stream	L1
6	RTP provides the facility of jitter _____ <b>a) media stream</b> b) expansion c) media modification d) security	L2
7	Which protocol provides the synchronization between media streams? a) RTP <b>b) RTCP</b> c) RPC d) RTCT	L3
8	An RTP session is established for _____ <b>a) each media stream</b> b) all media streams c) some predefined number of media streams d) no media stream	L5

**NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY, THENI.**

<b>Course/Branch</b> : B.E /ECE	<b>Year / Semester</b> :IV/VII	Format No.	NAC/TLP-07a.13
<b>Subject Code</b> :EC 8702	<b>Subject Name</b> :Adhoc Wireless Sensor Networks	Rev. No.	02
<b>Unit No</b> :5	<b>Unit Name</b> : Sensor Network Platforms And Tools	Date	30.09.2020

**OBJECTIVE TYPE QUESTION BANK**

9	Which one of the following multimedia formats can not be supported by RTP? a) MPEG-4 b) MJPEG c) MPEG <b>d) TXT</b>	L6
10	An RTP header has a minimum size of _____ <b>a) 12 bytes</b> b) 16 bytes c) 24 bytes d) 32 bytes	L6
11	Which one of the following is not correct? a) RTCP provides canonical end-point identifiers to all session participants b) RTCP reports are expected to be sent by all participants c) RTCP itself does not provide any flow encryption or authentication methods <b>d) RTCP handles the actual data delivery</b>	L3
12	Which protocol defines a profile of RTP that provides cryptographic services for the transfer of payload data? <b>a) SRTP</b> b) RTCP c) RCP d) RTCT	L4
13.	An RPC (remote procedure call) is initiated by the _____ a) server <b>b) client</b> c) client after the sever d) a third party	L4
14	In RPC, while a server is processing the call, the client is blocked _____ <b>a) unless the client sends an asynchronous request to the server</b> b) unless the call processing is complete c) for the complete duration of the connection d) unless the server is disconnected	L2
15.	A remote procedure call is _____ <b>a) inter-process communication</b> b) a single process c) a single thread d) a single stream	L1
16.	RPC allows a computer program to cause a subroutine to execute in _____ a) its own address space <b>b) another address space</b> c) both its own address space and another address space d) applications address space	L3
17.	RPC works between two processes. These processes must be _____	L5

**NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY, THENI.**

<b>Course/Branch</b> : B.E /ECE	<b>Year / Semester</b> :IV/VII	Format No.	NAC/TLP-07a.13
<b>Subject Code</b> :EC 8702	<b>Subject Name</b> :Adhoc Wireless Sensor Networks	Rev. No.	02
<b>Unit No</b> :5	<b>Unit Name</b> : Sensor Network Platforms And Tools	Date	30.09.2020

**OBJECTIVE TYPE QUESTION BANK**

	<p>a) on the same computer                  b) on different computers connected with a network  <b>c) on the same computer and also on different computers connected with a network</b>                  d) on none of the computers</p>	
18.	<p>A remote procedure is uniquely identified by _____                  a) program number                  b) version number                  c) procedure number  <b>d) all of the mentioned</b></p>	L3
19.	<p>An RPC application requires _____                  a) specific protocol for client server communication                  b) a client program                  c) a server program  <b>d) all of the mentioned</b></p>	L3
20.	<p>RPC is used to _____                  a) establish a server on remote machine that can respond to queries                  b) retrieve information by calling a query  <b>c) establish a server on remote machine that can respond to queries and retrieve information by calling a query</b>                  d) to secure the client</p>	L4
21.	<p>RPC is a _____  <b>a) synchronous operation</b>                  b) asynchronous operation                  c) time independent operation                  d) channel specific operation</p>	L2
22.	<p>The local operating system on the server machine passes the incoming packets to the _____  <b>a) server stub</b>                  b) client stub                  c) client operating system                  d) client process</p>	L5
23.	<p>One of the most obvious places to put an IDS sensor is near the firewall. Where exactly in relation to the firewall is the most productive placement?  <b>a) Inside the firewall</b>                  b) Outside the firewall                  c) Both inside and outside the firewall                  d) Neither inside the firewall nor outside the firewall.</p>	L5
24.	<p>What is the purpose of a shadow honeypot?                  a) To flag attacks against known vulnerabilities                  b) To help reduce false positives in a signature-based IDS  <b>c) To randomly check suspicious traffic identified by an anomaly detection system</b>                  d) To enhance the accuracy of a traditional honeypot</p>	L2

**NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY, THENI.**

<b>Course/Branch</b> : B.E /ECE	<b>Year / Semester</b> :IV/VII	Format No.	NAC/TLP-07a.13
<b>Subject Code</b> :EC 8702	<b>Subject Name</b> :Adhoc Wireless Sensor Networks	Rev. No.	02
<b>Unit No</b> :5	<b>Unit Name</b> : Sensor Network Platforms And Tools	Date	30.09.2020

**OBJECTIVE TYPE QUESTION BANK**

25	At which two traffic layers do most commercial IDSes generate signatures? a) Application layer and Network layer b) Network layer and Session Layer c) Transport layer and Application layer <b>d) Transport layer and Network layer</b>	L1
26	IDS follows a two-step process consisting of a passive component and an active component. Which of the following is part of the active component? a) Inspection of password files to detect inadvisable passwords <b>b) Mechanisms put in place to reenact known methods of attack and record system responses</b> c) Inspection of system to detect policy violations d) Inspection of configuration files to detect inadvisable settings	L4
27	When discussing IDS/IPS, what is a signature? a) An electronic signature used to authenticate the identity of a user on the network <b>b) Attack-definition file</b> c) It refers to “normal,” baseline network behavior d) It is used to authorize the users on a network	L2
28	“Semantics-aware” signatures automatically generated by Nemean are based on traffic at which two layers? a) Application layer and Transport layer b) Network layer and Application layer c) Session layer and Transport layer <b>d) Application layer and Session layer</b>	L2
29	Which of the following is used to provide a baseline measure for comparison of IDSes? <b>a) Crossover error rate</b> b) False negative rate c) False positive rate d) Bit error rate	L3
30	Which of the following is true of signature-based IDSes? a) They alert administrators to deviations from “normal” traffic behavior b) They identify previously unknown attacks c) The technology is mature and reliable enough to use on production networks <b>d) They scan network traffic or packets to identify matches with attack-definition files</b>	L4