Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2020

Course:	**IT Systems Security**	**Semester:**	**VI**
Course Code:	**CSSF3005**	**Programme:**	**B.Tech (CSE+CSF)**
Max. Marks:	**100**		
Instructions:			

Question	Which of the following is an advantage of anomaly detection?
Answer	a. Rules are easy to define. b. Custom protocols can be easily analyzed. c. The engine can scale as the rule set grows. d. Malicious activity that falls within normal usage patterns is detected.

Question	A false positive can be defined as…
Answer	a. an alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior. b. an alert that indicates nefarious activity on a system that is not running on the network. c. the lack of an alert for nefarious activity. d. Both a. and b.

Question	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?
Answer	a. Inside the firewall b. Outside the firewall c. Both None

Question	At which two traffic layers do most commercial IDSes generate signatures?
Answer	a. application layer b. network layer c. session layer d. Physical Layer

Question	When discussing IDS/IPS, what is a signature?

Answer	a. An electronic signature used to authenticate the identity of a user on the network b. Attack-definition file c. It refers to "normal," baseline network behavior d. None of the above

Question	Which of the following is used to provide a baseline measure for comparison of IDSes?
Answer	a. crossover error rate b. false negative rate c. false positive rate d. bit error rate

Question	If you have more than one computer connected in the home, it is important to protect every computer. You should have a ____firewall (such as a router) to protect your network:
Answer	a) Hardware b) Software c) HTML d) None of These

Question	Which among the following is correct:
Answer	a) Network firewalls are a software appliance running on general purpose hardware or hardware based firewall computer appliances that filter traffic between two or more networks. b) Host - based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine c) Both of Above d) None of These

Question	Application layer firewalls works on the application level of the ____stack (i.e. all browser traffic or all telnet or FTP traffic) and may intercept all packets travelling to or from an application:
Answer	a) TCP b) IP c) Both of Above d) None of These

□

Question	Which among the following is correct characteristics about proxy server:
Answer	a) A proxy server may act as a firewall by responding to input packets in the manner of an application while blocking other packets. b) A proxy server is a gateway from one network to another for a specific network application c) It performs its tasks or functions as a proxy on behalf of the network user; d) All of the Above

Question	In order to interpret XML documents one should
Answer	a. Use standardized tags b. Have a document type definition which defines the tags c. Define the tags separately d. Specify tag filename

□

Question	A search engine is a program to search
Answer	a. for information b. web pages c. web pages for specified index terms d. web pages for information using specified search terms

☑

Question	Which of the following does NOT use a 'Cryptographical Technique' to protect data?
Answer	a. the use of digital signatures b. data encryption ✓ c. the use of stored encrypted password files d. using asymmetric keys at 'sender' and 'receiver' nodes

□

Question	1. Why are traditional authentication methods unsuitable for use in computer networks?
Answer	✓ a. they do not use cryptographical techniques b. they do not permit high speed data flow c. they use passwords d. they are incompatible with the internet

Question	1. What is the main purpose of access control?
Answer	a. to authorise full access to authorised users ✓ b. to limit the actions or operations that a legitimate user can perform c. to stop unauthorised users accessing resources d. to protect computers from viral infections

Question	1. Which of the following is NOT a good property of a firewall?
Answer	a. only authorised traffic must be allowed to pass through it b. the firewall itself, should be immune to penetration c. it should allow for easy modification by authorised users d. traffic must only be allowed to pass from inside to outside the firewall

□

Question	1. ______ This is a protocol that a proxy server can use to accept requests from client users in a company's network sothat it can forward them across the Internet.
Answer	

	a) socks b) bottleneck c) Telnet d) AUP

Question	1. What is the use of Bridge in Network?
Answer	✓ to connect LANS to separate LANs to control Network Speed All of the above

Question	1. What is logical security?
Answer	Logical security means using common sense, and not being paranoid in relation to security measures. Logical security is to secure rooms with servers, so that they are not available for access (such as locks and alarms). c. Logical security is to have measures to stop the attack of the network via cables (electronic). d. Logical security is a firewall method.

Question	1. What do we mean by the top corner of the security triangle (integrity)? a.
Answer	That one is sure that the information is correct and that the source of information is as specified. b. That one is a sure that no unauthorized persons get access to the information.

	c. The extent to which information is available. d. That one is a sure that information does not harm the business.

Question	Using public key cryptography, X adds a digital signature to message M, encrypts < M, >, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations?
Answer	Encryption: X’s private key followed by Y’s private key; Decryption: X’s public key followed by Y’s public key Encryption: X’s private key followed by Y’s public key; Decryption: X’s public key followed by key Encryption: X’s public key followed by Y’s private key; Decryption: Y’s public key followed by X’s private key Encryption: X’s private key followed by Y’s public key; Decryption: Y’s private key followed by X’s public key

□

Question	Suppose that everyone in a group of N people wants to communicate secretly with the N–1 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is
Answer	✓ 2N N(N-1) N(N-1)/2 (N – 1)2

Question	Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires
Answer	✓ Anarkali’s public key. Salim’s public key. Salim’s private key Anarkali’s private key.

Question	Which of the following is not one of the functions of a digital signature?
Answer	verification of the sender prevention of the sender from disowning the message prove the integrity of the message ✓ protect the public key

Question	The minimum positive integer p such that 3p modulo 17 = 1 is
Answer	5 8 12 16

Question	Does socket programming support multi-programming?
Answer	✓ Yes No May ben be ca

□

Question	When a UDP segment arrives at a host, in order to direct the segment to the appropriate socket, the operating system's network stack uses the following fields: (circle ALL that are true – 2 points) When a UDP segment arrives at a host, in order to direct the segment to the appropriate socket, the operating system's network stack uses the following fields: (circle ALL that are true – 2 points) (a) the source IP address. (b) the destination IP address (c) the source port number (d) the destination port number When a UDP segment arrives at a host, in order to direct the segment to the appropriate socket, the operating system's network stack uses the following fields: (circle ALL that are true – 2 points) (a) the source IP address. (b) the destination IP address (c) the source port number (d) the destination port number When a UDP segment arrives at a host, in order to direct the segment to the appropriate socket, the operating system's network stack uses the following fields: (circle ALL that are true – 2 points) (a) the source IP address. (b) the destination IP address (c) the source port number (d) the destination port number

□

Question	Which is true of the UNIX Socket API?
Answer	(a) If a chunk of data written to a TCP socket is smaller than the MSS, it will all be sent in the same packet. ✓ (b) Writing a single message to a UDP socket can result in the network stack sending multiple packets. (c) The socket allocated by the accept() system call is assigned a new port number ✓ (d) You can call connect() on a UDP socket

□

Question	Which of the following are type of valid environments for socket programming?
Answer	Proxy ✓ Iterative Virtual Multi-threader

□

Question	Is there any error in following code: import socket #for sockets import sys #for exit try: #create an AF_INET, STREAM socket (TCP) sock_obj = socket.socket(socket.AF_INET, socket.SOCK_STREAM) except socket.error as err_msg: print ('Unable to instantiate socket. Error code: ' + str(err_msg[0]) + ' , Error message : ' + err_msg[1]) sys.exit(); print ('Socket Initialized')
Answer	True ✓ False

□

6. ↕ Multiple Choice: 9: Which methods are commonly used in Se...

Points:1

Question	Which methods are commonly used in Server Socket class?
Answer	a) Public Output Stream get Output Stream () ✓ b) Public Socket accept () c) Public synchronized void close ()

	d) None of the mentioned

□

Question	The client in socket programming must know which information?
Answer	a) IP address of Server b) Port number ✓ c) Both IP address of Server & Port number d) None of the mentioned

Question	The URL Connection class can be used to read and write data to the specified resource referred by the URL
Answer	✓ True False

Question	Datagram is basically an information but there is no guarantee of its content, arrival or arrival time.
Answer	✓ True False

Question	The flush () method of Print Stream class flushes any un cleared buffers in memory
Answer	✓ True False

Question	Which classes are used for connection-less socket programming?
Answer	a) Datagram Socket b) Datagram Packet ✓ c) Both Datagram Socket & Datagram Packet d) None of the mentioned

□

12. ↕ True / False: 19: There is error in following code: ...

Points:1

Question	There is error in following code:

	import socket ip = socket.gethostbyname('www.google.com') print ip
Answer	True ✓ False

Question	Which of the following database security mechanisms uses public-key and private-key cryptography to encrypt all connections between caller and listener
Answer	✓ IP Sec security Content-based firewalls SSL connection A demilitarised zone(DMZ)
In	

□

14. ↕ Multiple Choice: 14: When we update any tuple in the relat...

Points:1

Question	When we update any tuple in the relation which Authorization on a relation allows a user to?
Answer	select authorization ✓ update authorization grant authorization define authorization
In	

Question	The grants privileges on SQL authorization mechanism doesn't have
Answer	Specified attributes Specified tuples Entire relation ✓ Entire relation None of the above
In	

□

16. ↕ Multiple Choice: 16: To represent both data and relationsh...

Points:1

Question	To represent both data and relationships among a collection of tables data is known as
Answer	Object-based Data model Entity-relationship model ✓ Relational Model

	Semi-structured data model
In	

□

17. ↕ Multiple Choice: 17: If a DNS server accepts and uses the ...

︾

Points:1

Question	If a DNS server accepts and uses the wrong details from a host that has no authority giving that information, then this technique is called …?
Answer	DNS hijacking DNS lookup ✓ DNS spoofing All of the above
In	

□

18. ↕ Multiple Choice: 18: A method that uses two independent pi...

︾

Points:1

Question	A method that uses two independent pieces/processes of information to identify a user is known as…
Answer	Authentication through encryption Password-method authentication Two-method authentication ✓ Two-factor authentication
In	

□

19. ↕ Multiple Choice: 19: Applications create queries dynamical...

︾

Points:1

Question	Applications create queries dynamically, can be considered as a risk source of
Answer	Active attacks Passive attacks Forgery ✓ Injection
In	

□

20. ↕ Multiple Choice: 20: What is one reason why successfully p...

︾

Points:1

Question	What is one reason why successfully prosecuting computer crimes is so challenging?
Answer	There is no way to capture electrical data reliably

	The evidence in computer cases does not follow best evidence directives. ✓ These crimes do not always fall into the traditional criminal activity categories. Wiretapping is hard to do legally
In	

□

21. ↕ Multiple Choice: 21: To better deal with computer crime, s...

⌄

Points:1

Question	To better deal with computer crime, several legislative bodies have taken what steps in their strategy?
Answer	Expanded several privacy laws ✓ Broadened the definition of property to include data Required corporations to have computer crime insurance Redefined transborder issues
In	

□

22. ↕ Multiple Choice: 22: Many privacy laws dictate which of th...

⌄

Points:1

Question	Many privacy laws dictate which of the following rules?
Answer	Individuals have a right to remove any data they do not want others to know. Agencies do not need to ensure that the data is accurate Agencies need to allow all government agencies access to the data. ✓ Agencies cannot use collected data for a purpose different from what it was collected for.
In	

□

23. ↕ Multiple Choice: 23: Which of the following is not true ab...

⌄

Points:1

Question	Which of the following is not true about dumpster diving?
Answer	It is legal. ✓ It is illegal. It is a breach of physical security. It is gathering data from places people would not expect to be raided.
In	

□

24. ↕ Multiple Choice: 24: If security was not part of the devel...

⌄

Points:1

Question	If security was not part of the development of a database, how is it usually handled?
Answer	Cell suppression Trusted back end ✓ Trusted front end Views
In	

□

25. ↕ Multiple Choice: 25: If one department can view employees'...

Points:1

Question	If one department can view employees' work history and another group cannot view their work history, what is this an example of?
Answer	Context-dependent access control Content-dependent access control Separation of duties Mandatory access control