aRlease fill out the next table with your answers of Parti-

b) SYN flood attack with changed pattern

Q. No.	Chosen Answer	Q. No.	Chosen Answer
1		111111	
2		12	
3		13	
4		14	
5		15	
6		16	9
7		17	
8		18	
9	8	19	
10		20	

	AND DESCRIPTION OF THE PARTY OF
7	7. (4) (4)
8	8
9	9
10	0
Part1. Choose the correct answer (20 pts: 1 ex	
1) Signal interception is a serious potential netwo	
a) Vulnerability	c) Fabrication d) Availability failure
b) Countermeasure	
2) Assume an attacker need to redirect a user to How this attack can be accomplished?	a malicious site.
a) Ping of death	c) Echo CharGen
b) DNS spoofing	d) Port scanning
3) is a virtual line that encircles a protect	cted set of computing resources:
a) Firewall	c) Security Perimeter
b) Virtual private network	d) Demilitarized Zone
4) prevents an eavesdropper from le transit in a network	earning the source, destination, or content of data in
a) SSL	c) Onion routing
b) Secure Shell	d) Link encryption
5) An attacker intercepts this stream of packet to be P1 P3 P2 P5 P4. What attack is launched here?	ets P1 P2 P3 P4 P5 , and modifies the order of packets
a) Replay	c) Insertion
b) Sequencing	d) Substitution
6) Encryption is not suitable for preventing v	which of the following threats:
	c) Replay attack
a) Interception	d) Eavesdropping
Man-in-the-middle Attack	•
) An example of an attack that can be detec	cted by Signature-Based intrusion detection:
	c) New attack with no signature
) Smurf attack	d) Attack generated from inside the netwo
avai good attack with changed pattern	<u> </u>

15) Which of the <u>firewall lim</u> its traffic based on p	packet header data: addresses and ports on
15) Which of the tirewatt minor	
a) Guard	c) Circuit level gateway d) Application proxy
b) Packet filtering 16) The necessary condition to apply the swapp	ing suppression technique is to:
a) Keep the same statical results b) Do the swap for a large number of rows	

- c) Keep the order of columns the same
- d) Keep the order of rows the same
- 17) Rule allows the internal traffic goes out through TCP/80 to the external network.

	ا _ ا	Source Address	Destination Address	Destination Port	Action
Rule	Туре	Address	1.75	25	Permit
1	TCP	•	192.168.1.*	_~_	_
<u>. </u>		•	192.168.1.*	69	Permit
2	UDP		172	100	Permit
3	TCP	192.168.1.*	•	80	14
	1.4	-	100,100 1 10	80	Permit
4	TCP	•	192.168.1.18	- W.	-

a) 1

b) 2

(c) 3

18) All security enforcement mechanisms reside in:

- (a) Security kernel
- b) Reference monitor

c) OS kernel

d) Microkernel

19) One of the trusted system characteristics concerned with preventing interference between a user and the security enforcement mechanisms of the operating system

- a) A trusted path
- b) A secure startup

c) Object reuse control

20) Suppose you need to know if your classmate Sara got A+ in CS 433.

Sara is a visiting student from Yanbu.

Since students' grades are sensitive information, you tried these two queries.

Count College=Yonbu & Major=CS & Course=433 & Section C9A Count College=Yonbu & Major=CS & Course=433 & Section C9A & Grade=A+

The results for these two queries were 2 and 4.

What type of disclosure have you tried here?

a) Probable value b) Aggregation

- c) Inference by arithmetic
- d) Bounds

- 8) You are allowed to use the copyrighted materials (e.g.: a novel) for:
- a) Research and Criticism
- Write another novel with a similar script
- c) Produce a film version of the book

c) Electronic wiretapping d) Cybercrime activates

- d) Use a few lines without a reference to the original author
- 9) Computer Fraud and Abuse Act prohibits:
- a) Trafficking in passwords
- b) Protects the privacy of personal data
- 10) Session Forgery violates:
- a) Confidentiality b) Integrity

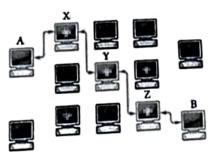
- c) Availability d) CIA
- 11) The encryption algorithm used in the $\overline{ ext{WEP}}$ protocol is:
- a) RC4
- b) RSA

- c) AES
- d) DE

a .. A & 5 184 :. 12

- 12) Which configuration this cipher suite TLS_RSA_WITH_AES_128_CBC_SHA represents:
- a) AES with 128-key authentication, RSA encryption, and SHA hash function b) RSA authentication, with no encryption, and SHA hash function
- c) RSA authentication, AES with 128-bit key encryption, and SHA hash function
- d) RSA authentication, AES with 128-bit key encryption, and MD5 hash function
- 13) uses short, infrequently changed encryption keys, it requires no authentication, and its integrity is easily compromised:
- a) WEP b) WPA

- c) SSH
- d) SSL
- 14) The sender A sends message M using onion routing to receiver B.
- Hence, M is encrypted under four different keys. The order of applying these keys is:



- a) M encrypted with X'PK, Y'PK, Z'PK, and B'PK
- M encrypted with A'PK, Z'PK, Y'PK, and X'PK b)
- M encrypted with B'PK, Y'PK, Z'PK, and X'PK d) M encrypted with B'PK, Z'PK, Y'PK, and X'PK

Part2.

21) Match each of the concepts with its definition (7 pts: 1 each)

***- ali	Definition
Attack 1-Session hijacking	a) The disruption of existing wireless communications 2
2-Forced Disassociation	b) The attacker allows an interchange to begin between two parties but then diverts the communication
3-Jamming	c) The attacker forced termination of the session
3-Jamining	d) Intercept all network communication

	Definition
Firewall	a) Judge according to information from multiple packets
1-Packet filtering	b) Implements any programmable set of conditions, even if the
2-Stateful inspection firewall	anditions become highly sophisticated.
3-A circuit-level gateway	c) Limits traffic based on packet header data: addresses and ports on
	packets d) Connects two separate subnetworks as if they were one
1-A guard	
	e) A program that runs on a single host to monitor and control traff
	to that host

22) Answer with True or False (3 pts: 1 each)

- a) If someone discovers a trade secret independently, it is considered an infringement.
- b) Patents law can protect algorithms, and the copyright designed to protect a software.
- The possible suppression of the Aggregation disclosure is by keeping track of what each user c) knows.

الله وال الله المنطر مها المناه المود المود المود

28) Assume you are STC's network administrator. You must enable users to access some of the company's resources, like the website server.

Thus, you are responsible for protecting sensitive resources like a database server.

How can you accomplish this security task?

29) Suppose you discovered a security flaw in Apple Pay with IOS 15.5 that attackers can use to access users' credit card information.

How should you report this flaw to Apple? Write all steps.

30) A Bonus question (2 pts)

a-How the network address translation works?

B-How does NAT provide security to the network?



- Fill in the Bl	ank Questions (4 pts: 1 each)
23) An intrusion	detection system	that tries to block or stop the attack is called 💆
		s the accidental attempt to send sensitive data where it is no
25) a	register that cont	tains a predefined memory address
26)is becomes part of		vare package that takes advantage of root status or effectively
B- Short Answ	ver Questions (6	pts: 2 each)
27) Examine the	e following packe	t fragments and follow the start and length instructions to
letermine whic	h of them can be	used to launch a teardrop attack?
Packet 1	Packet 2	Packet 3
Start>10 Jength=50	Start=10 Jeogth=50	Stati>20 Sength=60
Start=60 length=20	Start=40 length=30	Staft=80 length=20
Start=80 length=10	Start=50 length=10	Start=100 length=10

arts.

aPlease fill out the next table with your answers of Parti-

Q. No.	Chosen Answer	Q. No.	Chosen Answer
1 1000		11	and the state of t
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9	1	19	N .
10		20	8

Part1. Choose the correct answer (20 pts; 1 each).

Replay

b) Sequencing

a) Interception

a) Smurf attack

b) Man-in-the-middle Attack

b) SYN flood attack with changed pattern

a)

1)	Signal interception is a serious potential network		•
	Vulnerability	•	Fabrication
ь)	Countermeasure	d)	Availability failure
	Assume an attacker need to redirect a user to a mow this attack can be accomplished?	alici	ous site.
a)	Ping of death	c)	Echo CharGen
b)	DNS spoofing	d)	Port scanning
3) .	is a virtual line that encircles a protected	set	of computing resources:
a)	Firewall	c	Security Perimeter
	Virtual private network	d) Demilitarized Zone
4)	prevents an eavesdropper from learn	ing	the source, destination, or content of data in
trai	nsit in a network		
1)	SSL		c) Onion routing
)	Secure Shell		d) Link encryption
be	an attacker intercepts this stream of packets P e P1 P3 P2 P5 P4. It attack is launched here?	1 P	2 P3 P4 P5, and modifies the order of packets

6) Encryption is not suitable for preventing which of the following threats:

7) An example of an attack that can be detected by Signature-Based intrusion detection:

c) Insertion

d) Substitution

c) Replay attack

d) Eavesdropping

c) New attack with no signature

d) Attack generated from inside the network

- 8) You are allowed to use the copyrighted materials (e.g.: a novel) for: Research and Criticism Write another novel with a similar script c) Produce a film version of the book d) Use a few lines without a reference to the original author
- 9) Computer Fraud and Abuse Act prohibits:
- a) Trafficking in passwords
- b) Protects the privacy of personal data
- 10) Session Forgery violates:
- a) Confidentiality
- b) Integrity

- c) Electronic wiretapping
- d) Cybercrime activates
- c) Availability
- d) CIA
- 11) The encryption algorithm used in the WEP protocol is:
- a) RC4
- b) RSA

- c) AES
- d) DE

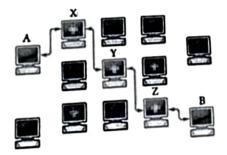
Rsq =- 9 a :. A E5 Key :. 12 hash 154

- 12) Which configuration this cipher suite TLS_RSA_WITH_AES_128_CBC_SHA represents:
- a) AES with 128-key authentication, RSA encryption, and SHA hash function
- b) RSA authentication, with no encryption, and SHA hash function
- c) RSA authentication, AES with 128-bit key encryption, and SHA hash function
- d) RSA authentication, AES with 128-bit key encryption, and MD5 hash function
- 13) uses short, infrequently changed encryption keys, it requires no authentication, and its integrity is easily compromised:
- a) WEP

c) SSH

b) WPA

- d) SSL
- 14) The sender A sends message M using onion routing to receiver B. Hence, M is encrypted under four different keys. The order of applying these keys is:



- a) M encrypted with X'PK, Y'PK, Z'PK, and B'PK
- b) M encrypted with A'PK, Z'PK, Y'PK, and X'PK c) M encrypted with B'PK, Y'PK, Z'PK, and X'PK
- d) M encrypted with B'PK, Z'PK, Y'PK, and X'PK

15) Which of the <u>(irewall limi</u> ts traffic based on	necket header data: addresses and ports on
(5) Which of the firewall limits traffic based on	packet near
packets:	c) Circuit level gateway d) Application proxy
b) Packet filtering 16) The necessary condition to apply the swapp	
Keep the same statical results Do the swap for a large number of rows Keep the order of columns the same	
d) Keep the order of rows the same 17) Rule allows the internal traffic goes	out through TCP/80 to the external network.

1 1	Source Address	Destination Address	Destination Port	Action	
Rule	Туре	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	192.168.1.*	25	Permit
ι	TCP	•			Permit
,	UDP	•	192.168.1.*	69	_
÷	-	192.168.1.*	•	80	Permit
3	TCP	192.100.11		80	Permit
4	TCP	•	192.168.1.18	- W.	-

a) 1

b) 2

(c) 3

18) All security enforcement mechanisms reside in:

a) Security kernel

c) OS kernel

b) Reference monitor

d) Microkernel

19) One of the trusted system characteristics concerned with preventing interference between a user and the security enforcement mechanisms of the operating system

a) A trusted path

c) Object reuse control

b) A secure startup

20) Suppose you need to know if your classmate Sara got A+ in CS 433.

Sara is a visiting student from Yanbu.

Since students' grades are sensitive information, you tried these two queries.

Count College=Yonbu & Major=CS & Course=433 & Section C9A Count College=Yonbu & Major=CS & Course=433 & Section C9A & Grade=A+

The results for these two queries were 2 and 4.

What type of disclosure have you tried here? a) Probable value

c) Inference by arithmetic

b) Aggregation

d) Bounds

Part2.

21) Match each of the concepts with its definition (7 pts: 1 each)

***- ali	Definition
Attack 1-Session hijacking	a) The disruption of existing wireless communications 2
2-Forced Disassociation	b) The attacker allows an interchange to begin between two parties but then diverts the communication
3-Jamming	c) The attacker forced termination of the session
3-Jamining	d) Intercept all network communication

	Definition
Firewall	a) Judge according to information from multiple packets
1-Packet filtering	b) Implements any programmable set of conditions, even if the
2-Stateful inspection firewall	anditions become highly sophisticated.
3-A circuit-level gateway	c) Limits traffic based on packet header data: addresses and ports on
	packets d) Connects two separate subnetworks as if they were one
1-A guard	
	e) A program that runs on a single host to monitor and control traff
	to that host

22) Answer with True or False (3 pts: 1 each)

- a) If someone discovers a trade secret independently, it is considered an infringement.
- b) Patents law can protect algorithms, and the copyright designed to protect a software.
- The possible suppression of the Aggregation disclosure is by keeping track of what each user c) knows.

الله وال الله المنطر مها المناه المود المود المود

28) Assume you are STC's network administrator. You must enable users to access some of the company's resources, like the website server.

Thus, you are responsible for protecting sensitive resources like a database server.

How can you accomplish this security task?

29) Suppose you discovered a security flaw in Apple Pay with IOS 15.5 that attackers can use to access users' credit card information.

How should you report this flaw to Apple? Write all steps.

30) A Bonus question (2 pts)

a-How the network address translation works?

B-How does NAT provide security to the network?



Part3.

A- Fill in the Blank Questions (4 pts: 1 each)

- 23) An intrusion detection system that tries to block or stop the attack is called
- 24) technique prevents the accidental attempt to send sensitive data where it is not allowed to go
- 25)..... a register that contains a predefined memory address
- 26) is a malicious software package that takes advantage of root status or effectively becomes part of the OS

B- Short Answer Questions (6 pts: 2 each)

27) Examine the following packet fragments and follow the start and length instructions to determine which of them can be used to launch a teardrop attack?

Packet 1	Packet 2	Packet 3
Start=10 Jeogth=50	Start=10	Start=20
	Jength 250	Seogth 603
Start=60	Start-At	
length=20	length=30	Jength-26
Start=80 length=10	Start=50 length=10	Start=100 length=10
Packet Figure	Packet Programmis	Packet Fragments