

Please fill out the next table with your answers of Part I:

Q. No.	Chosen Answer	Q. No.	Chosen Answer
1		11	
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

Part I. Choose the correct answer (20 pts: 1 each).

1) Signal interception is a serious potential network

- a) **Vulnerability**
- b) Countermeasure
- c) Fabrication
- d) Availability failure

2) Assume an attacker need to redirect a user to a malicious site. How this attack can be accomplished?

- a) Ping of death
- b) **DNS spoofing**
- c) Echo CharGen
- d) Port scanning

3) is a virtual line that encircles a protected set of computing resources:

- a) Firewall
- b) Virtual private network
- c) **Security Perimeter**
- d) Demilitarized Zone

4) prevents an eavesdropper from learning the source, destination, or content of data in transit in a network

- a) SSL
- b) Secure Shell
- c) **Onion routing**
- d) Link encryption

5) An attacker intercepts this stream of packets P1 P2 P3 P4 P5 , and modifies the order of packets to be P1 P3 P2 P5 P4.

What attack is launched here?

- a) Replay
- b) **Sequencing**
- c) Insertion
- d) Substitution

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

- a) Interception
- b) **Man-in-the-middle Attack**
- c) Replay attack
- d) Eavesdropping

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

- a) Smurf attack
- b) SYN flood attack with changed pattern
- c) New attack with no signature
- d) **Attack generated from inside the network**

15) Which of the firewall limits traffic based on packet header data: addresses and ports on packets:

- a) Guard
- b) **Packet filtering**
- c) Circuit level gateway
- d) **Application proxy**

16) The necessary condition to apply the swapping 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.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit

- a) 1
- b) 2
- c) **3**
- d) 4

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**
- d) Audit

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
- b) 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
- c) Electronic wiretapping
- d) Cybercrime activates

10) Session Forgery violates:

- a) Confidentiality
- b) Integrity
- c) Availability
- d) CIA

11) The encryption algorithm used in the WEP protocol is:

- a) RC4
- b) RSA
- c) AES
- d) DE

Rsa = -4 a: AES key: 12 hash: SHA

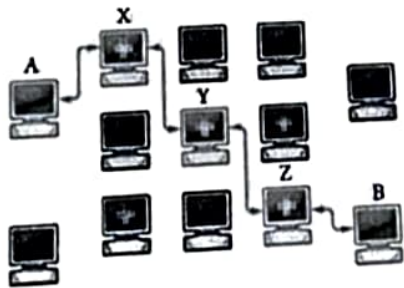
12) Which configuration this cipher suite TLS_RSA_WITH_AES_128_CBC_SHA represents:

- 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
- 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

Part 2.**21) Match each of the concepts with its definition (7 pts: 1 each)**

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

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

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

- If someone discovers a trade secret independently, it is considered an infringement.
- 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 knows.

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?

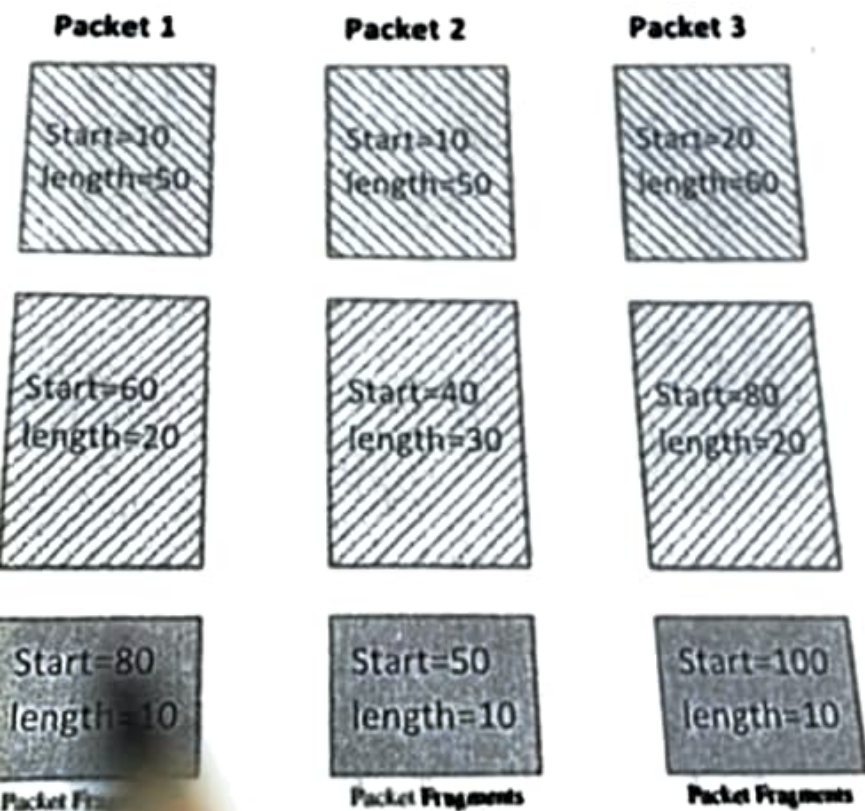


A- Fill in the Blank Questions (4 pts: 1 each)

- 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?



Please fill out the next table with your answers of Part I:

Q. No.	Chosen Answer	Q. No.	Chosen Answer
1		11	
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

Part I. Choose the correct answer (20 pts: 1 each).

1) Signal interception is a serious potential network

- a) Vulnerability
- b) Countermeasure
- c) Fabrication
- d) Availability failure

2) Assume an attacker need to redirect a user to a malicious site. How this attack can be accomplished?

- a) Ping of death
- b) DNS spoofing
- c) Echo CharGen
- d) Port scanning

3) is a virtual line that encircles a protected set of computing resources:

- a) Firewall
- b) Virtual private network
- c) Security Perimeter
- d) Demilitarized Zone

4) prevents an eavesdropper from learning the source, destination, or content of data in transit in a network

- a) SSL
- b) Secure Shell
- c) Onion routing
- d) Link encryption

5) An attacker intercepts this stream of packets P1 P2 P3 P4 P5 , and modifies the order of packets to be P1 P3 P2 P5 P4.

What attack is launched here?

- a) Replay
- b) Sequencing
- c) Insertion
- d) Substitution

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

- a) Interception
- b) Man-in-the-middle Attack
- c) Replay attack
- d) Eavesdropping

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

- a) Smurf attack
- b) SYN flood attack with changed pattern
- 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:

- a) Research and Criticism
- b) 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
- c) Electronic wiretapping
- d) Cybercrime activates

10) Session Forgery violates:

- a) Confidentiality
- b) Integrity
- c) Availability
- d) CIA

11) The encryption algorithm used in the WEP protocol is:

- a) RC4
- b) RSA
- c) AES
- d) DE

*RSA = 2-4 a: AES key: 12
hash: SHA*

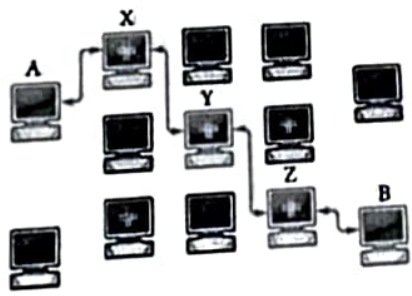
12) Which configuration this cipher suite TLS_RSA_WITH_AES_128_CBC_SHA represents:

- 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
- 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 firewall limits traffic based on packet header data: addresses and ports on packets:

- a) Guard
- b) Packet filtering
- c) Circuit level gateway
- d) Application proxy

16) The necessary condition to apply the swapping 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.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit

- a) 1
- b) 2
- c) 3
- d) 4

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
- d) Audit

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

Part 2.**21) Match each of the concepts with its definition (7 pts: 1 each)**

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

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

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

- If someone discovers a trade secret independently, it is considered an infringement.
- 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 knows.

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?

