1. A spy reads and alters Bob's to Alice's message. Which security goal is threatened by this attack?

   (0.5/0.5 Points)

   ○ Integrity

   ○ Non repudiation

   ○ Privacy

   ○ Repudiation

   ○ 1 and 2

   ◉ 1 & 3 ✓

   ○ 1&4

   ○ 2 & 3

   ○ 3 & 4

2. In Non-conventional cryptosystems ---------- keys exist for signature verification
   (0.5/0.5 Points)

   ○ 4

   ○ 3

   ◉ 1 ✓

   ○ 2

   ○ none of the above

   ○ 3 & 4

3. When a network administrator sends update message to hosts and host acknowledged after receipt using wireless mode of communication,----------- authentication to be done
   (0.5/0.5 Points)

   ○ Mutual

   ◉ Data origin ✓

   ○ Zero Knowledge

   ○ Two way

4. ------------ is a irreversible
(0.5/0.5 Points)

○ Playfair

○ Ciphering

● Hashing ✓

○ Mediation

○ Fielstel network

5. In ceaser cipher, if plaintext= ciphertext, then key is
(0.5/0.5 Points)

● 0 ✓

○ 1

○ 2

○ 3

○ 4

6. What kind of cryptosystem is possible to develop?
(0.5/0.5 Points)

○ Unconditional & secure

● Computational & secure ✓

○ Playfair secure

○ Monoalpahbetical secure

○ Non breakable

7. In symmetric key encryption using -------key, authentication can be achieved.
(0.5/0.5 Points)

○ 0

● 1 ✓

○ 2

○ 3

○ 4

8. DOS influences ---------of information.
   (0.5/0.5 Points)

   ○ Integrity

   ○ Privacy

   ◉ Availability ✓

   ○ Repudiation

   ○ Non repudiation

   ○ Mediation

   ○ Granularity

9. An example for symmetric cryptosystem is ----------
   (0.5/0.5 Points)

   ○ SHA

   ○ RSA

   ○ RABIN

   ◉ None of the above ✓

10. An unauthorized person learns the existence of a piece of data is ------------violation
    (0.5/0.5 Points)

    ○ Integrity

    ○ Non Repudiation

    ◉ Privacy ✓

    ○ Repudiation

    ○ Non availability

11. -------------------- provides a standard measurement system that allows accurate and consistent scoring of vulnerability impact.
(0.5/0.5 Points)

- ◉ CVSS ✓

- ○ CVE

- ○ P table

- ○ S-box

- ○ Access List

- ○ Reference Monitor

- ○ Access Log

12. --------------- not maintains multiple separate user profiles.
(0.5/0.5 Points)

- ○ Access List

- ◉ Federated Identity service ✓

- ○ SSO

13. -----------is a row of access control matrix
    (0.5/0.5 Points)

- ◉ Directory ✓

- ○ Dictionary

- ○ Granularity

- ○ Reference monitor

- ○ Object

- ○ Subject.

- ○ PKI

- ○ Certificate

14. The measure of mountable attack can be through-----------
    (0.5/0.5 Points)

- ○ Round Function

- ○ RCon Table

- ◉ Work factor ✓

- ○ Confusion & Diffusion

- ○ Substitution

- ○ Permutation

- ○ Shift Rows function

- ○ Shift Columns function

15. In ------------cipher, several plaintext alphabets decide encrypted text
    (0.5/0.5 Points)

○ Stream

○ Hashing

○ Playfair cipher

● Block ✓

○ All the above

○ None of the above

○ Blake

16. Alice wants to send an message with forgeable resistant, authentic, non-changed , and reusable free properties are kept in mind. What is your suggestion for him?
    (0.5/0.5 Points)

○ Hashing

○ Encryption

● Signature ✓

○ KDC

○ Certificates

○ mediation

17. A completely mediation system should fulfil ------------ properties.
    (0.5/0.5 Points)

○ 1

○ 2

● 3 ✓

18. A program with a file name "UPDATE_system_Time" does some changes in OS settings is an example of ------------
(0.5/0.5 Points)

○ Virus

○ Worm

◉ Trojan horse ✓

○ Bot

○ Threat

○ Ransomware

19. A symmetric encryption system is ------------ compared to asymmetric system W.R.T time
(0.5/0.5 Points)

◉ Fast ✓

○ Slow

○ Equal

20. -------------is an legal activity with a team of experts.
(0.5/0.5 Points)

○ Interception

○ Interruption

○ Fabrication

◉ Tiger Team analysis ✓

○ Cryptanalysis

1. MAC provides following services
   (1/1 Point)

   ○ privacy & integrity

   ○ integrity & non repudiation

   ○ Privacy and Signature

   ○ Non repudiation and Privacy

   ◉ Integrity& authentication ✓

   ○ integrity and non repudiation

   ○ authentication &

2. Browser Security can be achieved through
   (1/1 Point)

   ○ AES

   ○ RSA

   ◉ SSL ✓

3. Which of the following is not a major part of wireless data frame
(0.5/0.5 Points)

- ⦿ Frame Direction ✓

- ◯ Frame Header

- ◯ Payload

- ◯ Frame Check Sequence

4. Which of the following uses RC4 encryption Algorithm?
(0.5/0.5 Points)

- ⦿ WEP

- ◯ WAP2

- ◯ WEP and WAP2

- ◯ None of the above

✕

5. ----------------is an unauthorized access point to your wireless network
(0.5/0.5 Points)

Rogue access point

Correct answers: Rogue access points

6. Which wireless network attack makes use of symbols to share knowledge about the location and details of access points
(0.5/0.5 Points)

Warchalking ✓

3. Which of the following is not Addressing Failures DoS attack
   (0.5/0.5 Points)

   ○ Rerouting

   ○ Source routing and address spoofing

   ○ Traffic redirection

   ◉ Physical disconnection ✓

4. --------------attack is a variation of ping attack
   (0/0.5 Points)

ICMP flood

5. In --------------attack the destination maintains a queue called the SYN_RECV connections,
   (0.5/0.5 Points)

Syn flood ✓

6. Which of the following is/are the root threats to availability 🔊
   (0.5/0.5 Points)

   ○ insufficient capacity; overload

   ○ blocked access

   ○ unresponsive component

   ◉ All of the above

3. People who infect machines to turn them into bots are called-----------
   (0.5/0.5 Points)

botmaster ✓

4. -------------are machines running pieces of malicious code under remote control.
   (0/0.5 Points)

Bots

   Correct answers: Zombies

5. In---------------encryption , data are encrypted just before the system places them on the physical communications link
   (0.5/0.5 Points)

link ✓

6. Which of the following DDOs attack measured in •Requests/secs
   (0.5/0.5 Points)

   ⦿ Application level ✓

   ◯ Protocol Based

   ◯ Volumetric

   ◯ None of the above

3. Which of the following services provided by the SSL Record Protocol for SSL connections
   (0.5/0.5 Points)

   ○ A. Confidentiality

   ○ B. Message Integrity

   ○ C. Availability

   ● Both A and B ✓

   ○ All (A,B and C)

   ○ None of the above

   ○ Both B and C

4. ----------------is a pair of protocols (versions 1 and 2) originally defined for Unix but now
   available under most operating systems.
   (0.5/0.5 Points)

SSH ✓

5. ---------------protocol is combination of HTTP & SSL/TLS to secure communications between
   browser & server.
   (0.5/0.5 Points)

HTTPS ✓

6. Identify whether the following statement is Ture or False
   SSL operates between applications (such as browsers) and the TCP/IP protocols
   (0.5/0.5 Points)

   ● True ✓

   ○ False

3. ----------------is a relationship between the two entities which are communicating in IPSec
   (0.5/0.5 Points)

Security association ✓

4. ------------------is an anonymous communication technique over a computer network
   (0.5/0.5 Points)

Onion routing ✓

5. Which of the following services are provided by Encapsulating Security Payload?
   (0/0.5 Points)

   ○ A. Confidentiality

   ○ B. Message Integrity

   ○ C. Authentication

   ◉ All of the above

   ○ Only A and B

   ○ Only A and C ✓

   ○ Only B and C

6. In -------------- mode IP header and Payload are encrypted
   (0.5/0.5 Points)

Tunnel ✓

3. -------------- firewalls judge according to information from multiple packets.
   (0/0.5 Points)

   Packet filtering

   Correct answers: Stateful inspection

4. In which of the following way/s Network Address Translation cannot be performed
   (0.5/0.5 Points)

   ○ One- to- One

   ○ Many-to-One

   ◉ Many-to-Many ✓

   ○ All of the above

5. File Transfer Protocol is an example of -------------------firewall.
   (0.5/0.5 Points)

   Stateless ✓

6. ----------------Proxies known as dynamic proxies.
   (0.5/0.5 Points)

   Adaptive ✓

3. Which of the following protocol provides data confidentiality and data integrity?
(0/0.5 Points)

- ⦿ PPTP
- ○ L2TP ✓
- ○ Both PPTP and L2TP
- ○ None of the above

✕

4. If a company has one or more remote locations that they wish to join in a single private network they can create a/an --------------------to connect LAN to LAN
(0/0.5 Points)

- ⦿ Remote access VPN
- ○ Intranet VPN ✓
- ○ Extranet VPN
- ○ None of the above

5. Which type of VPN is used in the following scenario?
When a company has close relationship with another company (for example a partner, supplier or customer) they can build a VPN that connects LAN to LAN and that allows all of the various companies to work in a shared environment.   📖
(0.5/0.5 Points)

- ⦿ Extranet VPN ✓
- ○ Internet VPN
- ○ Remote Access VPN
- ○ None of the above

6. Which of the following component/s is/are required by Remote access VPN?
(0.5/0.5 Points)

- ○ Client Software
- ○ Network Access Server
- ⦿ Both A and B ✓
- ○ None of the above

3. With respect to computing locations, which of the following IDS is suitable for multi-layer network architecture?
(0.5/0.5 Points)

○ Independent

○ Stand-Alone

◉ Hierarchical ✓

○ None of the above

4. ---------IDS is OS specific
(0.5/0.5 Points)

○ Network Based

◉ Host based ✓

○ Both Network based and Host based

○ None of the above

✕

5. --------------------IDS uses predefined attack patterns
(0/0.5 Points)

○ A. Anomaly based

○ B. Signature Based ✓

◉ Both A and B

○ None of the above

6. ------------------uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
(0.5/0.5 Points)

◉ Network Based IDS ✓

○ Host Based

○ Both Network based and host based

○ None of the above

3. In which of the following risk analysis numbers can be assigned to various risks? 🔊
   (0.5/0.5 Points)

   ○ Qualitative

   ◉ Quantitative ✓

   ○ Mixed

   ○ None of the above

4. --------------------involves a set of actions to reduce or eliminate the risk.
   (0.5/0.5 Points)

   ◉ Risk Control ✓

   ○ Risk Impact

   ○ Risk Exposure

   ○ None of the above

5. If the likelihood of virus attack is 0.3 and the cost to clean up the affected files is $1000, then the risk exposure is ---------------

   🔊
   (0.5/0.5 Points)

   ○ $1000

   ◉ $300 ✓

   ○ $3000

   ○ None of the above

   ✕

6. Identify whether the following statement is True or False.
   If the leverage value of a proposed action is high enough, then we look for alternative but less costly actions or more effective reduction techniques.
   (0/0.5 Points)

   ◉ True

   ○ False ✓