SECTION A

1. Some sniffers perform DNS lookups in order
   * 1. To spread viruses
     2. To detect hackers and spammers operating on a network
     3. To replace IP address in their logs with fully quail
     4. To harvest passwords
2. The Source Route method is used to
   * 1. Locate sniffers on nearby network segments
     2. De-activate sniffers on a network
     3. E-direct all sniffing activities on the firewall of a network
     4. To protect a network from virus attacks
3. The decoy method of detecting sniffers on a network
   * + 1. Involves setting up a client and server on either side of the network
       2. The Server is configured with accounts that do not have rights or privileges
       3. Involves configuring firewalls to attack hackers
       4. Involves backing up all files on the main server with the network
   1. I and II b) II, III, and IV c) II and III d) I, II, III and IV
4. The command ----------- can be used to check if a sniffer is being run in a promiscuous mode
   1. -/ der config – d
   2. -/ if config – a
   3. -/ ps aux – a
   4. –c /-ip config – d
5. Motivation for hacking includes
   * + 1. Desire for recognition or fame
       2. Desire to spread spam or virus
       3. Revenge
       4. Intent to commit industrial, espionage
   1. I and II b)I, II, III c)II, III, IV d) I, II, III, IV
6. An ethical hacker is
   1. A security professional who applies his or her hacking skills for defensive purposes
   2. One who uses his or her hacking skills for teaching others how to hack
   3. A hacker who distributes Trojans and worms on the world
   4. A hacker who hacks only attacks of secure networks
7. Black hackers are well versed hackers who hacks websites and networks that
   1. Display valuable information
   2. Display information with a bad intent
   3. Hack with good intent
   4. Hacks sites with insufficient information
8. Sniffers are not easily detected when in operation and can be implemented from
   * + 1. Any computer within a network
       2. At the gateway
       3. At the routers
       4. When the link from the network to the internet is by wireless
   1. I b) I and II c)I, II and III d)I, II, III, IV
9. Sniffers look only at the traffic passing through the
   1. Network interface adaptor on the machine the application is running on
   2. Network adaptor and the RAM on the machine the sniffer is resident on
   3. Data passing through the buffer unit of the computer
   4. Hard disk in the machine the sniffer in running on
10. To spoof a trusted machine relationship, the attacker must
    * + 1. Identify the target pair of trusted machines
        2. Anesthetize the host the attacker intends to impersonate
        3. Forge the address of the host the attacker is pretending to be
        4. Accurately guess the correct sequence of all TCP/IP transmissions
    1. I and II only b) II, III and IV only c) III and IV d) I,II, III and IV
11. In an IP spoofing attack a tangible loss may occur when
    1. Spam or SYN flooding occur on the network under attack
    2. Valuable data is lost or duplicated
    3. The network is slowed down by the attacker
    4. The reputation of the victim is compromised
12. Blind spoofing is a kind of spoofing attack when the
    1. Hacker is not aware of all network conditions but uses various means to gain access to the network
    2. When the victim is not aware that he or she is being hacked
    3. The victim’s firewall cannot detect the attacker
    4. Attacker can attack the victim without being detected
13. Which of the following is an example of a damage caused by Trojan horse attack?
    * + 1. Erasing or overwriting data on the affected computer
        2. Re-installing itself after being disabled
        3. Copying fake links which will lead to false websites or chats and other accounts based websites
        4. Rewriting the URL of the victims address
      1. I and II b) II, III and IV c)I, II, III and IV d)I, II and III
14. A Trojan horse attack can be cleared by using
    * + 1. Antivirus software
        2. Booting the computer from a live CD and then using an antivirus afterwards
        3. Resetting jumpers on the hard disk and rebooting the whole computer
        4. Updating the firewall and testing whether the computer can be attacked
      1. I and II b) II and IV c) II only d) II, III and IV
15. The best way to clean a computer which has been heavily infested by a virus is to
    1. Reformat the hard disk and reinstall the operating system
    2. Clean the computer with an antivirus
    3. Prevent other users from using the affected files
    4. Delete all unfamiliar files on the hard disk
16. Various defences against man-in-the middle attacks use authentication techniques based on
    * + 1. Public key and secret key infrastructure
        2. Avoiding the use of wireless as a medium of transmission
        3. Use of strong passwords
        4. Off channel verification
      1. I b)II, III c) III, IV d) I, IV
17. ------------- enables closed-from solution to security that works well when only a single well-characterized property can be isolated as critical
    1. Breaking the system up into smaller components
    2. Zipping files
    3. Using a powerful firewall
    4. Using intelligent switches and routes
18. -------------- are computers that can either intentionally or unintentionally left vulnerable to attack by crackers
    1. Secure systems
    2. Operating systems
    3. Honey pots
    4. Proxies
19. In an active spoofing attack, the hacker can
    * + 1. See all the computers that reside on the victim’s network
        2. Hacker can hack an unsecured document on victims computer
        3. Hacker can guess all sequence numbers of all TCP/IP transmissions
        4. Hacker can see both parties and perform exploits such as sniffing data, corrupting data and all the contents of a packet
      1. I, II b) II, III c) I, IV d) II, III, IV
20. ARP (Address Resolution Protocol) spoofing attacks involves
    * + 1. Detecting broadcasts, faking the IP address and responding with a MAC address of the hacker’s computer
        2. Deleting the address of the victim’s computer
        3. Replacing the IP address of the victim’s with the victims host address
        4. Copying the password of the victim’s computer
      1. I, II b) II, III, IV c) I only d) I, IV
21. In a web spoofing attack, a hacker spoofs
    * + 1. The address of the host’s router and the gateway
        2. The hacker redirects all information meant for the victim on to a virtual server
        3. Spoofs an IP address through a website and also acquire a certificate used by a website
        4. Freezes the victims website
      1. I, II b) I, II, III c) II, III, IV d) II, III
22. In a DNS spoofing on a website, the hacker changes its website’s IP address to the IP address of
    1. I and II b) I, I and III c) II, III, IV d) I, II, III and IV
23. An apsend which is a spoofing tool, can perform
    * + 1. SYN flood attack
        2. UDP flood attack
        3. Ping attack
        4. Time-to-Live attack
      1. I and II b) I, II and III c) II, III, IV d)I, II, III and IV
24. Baiting as means to execute an attack relies mainly on
    1. The skill of the attacker
    2. The intensity of spam or flooding sent by an attacker
    3. Curiosity or the greediness of the attacker
    4. The efficiency of the firewall on the victims network
25. In a Quid pro quo attack, the attacker -----------
    1. Helps solve a problem and in the process have the user type a command that gives the attacker access to launch a malware attack
    2. Just launch a malware attack
    3. The victim stuns and anesthetize the attackers computer
    4. The attacker sends a bait by means of a Trojan horse and the launch a man-in-the-middle attack
26. In a man-in-the-middle attack the attacker
    1. attacks computers that are centrally place within a network
    2. The attacker attacks the hard disk and the network interface card of the victims computer
    3. The attacker eavesdrops, connect to the victim’s computer relays and alters data transmitted between workstations
    4. Disable all the computers on a network
27. --------------- is a form of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host’s machine
    1. Eaves dropping
    2. Flooding
    3. Spamming
    4. Trojan horse
28. Which of the following is a type of Trojan horse payload
    * + 1. Remote accessing
        2. Data destruction and security software disabler
        3. Downloader
        4. Denial-of-service attack
      1. I and II b)I,II and III c)II, III and IV d) I, II, III and IV
29. In an Address Resolution Protocol test, the windows driver for the network interface card
    1. Detects all hackers on the system
    2. Detects IP addresses of all computers attached to the network
    3. Examine the contents of the hard disk of the main server for the network
    4. Examines only the first octet of the MAC address
30. A firewall cannot recognize and detect internal attacks because
    1. Not all firewall are reliable
    2. Some hackers can by-pass a firewall
    3. Firewalls can detect internal intrusive attacks if only a proxy server is present in he network
    4. Firewall sit on the boundaries of networks
31. Which of the following commands can be used to detect a recently modified files on a server
    1. $find/-ctime-1-print
    2. $$find /-cdetect-1-detect
    3. $ find/-cdisallow-1-detect
    4. $deny/-ctime-1-intrusion
32. In the verification of the application layer protocols method as a means for signature recognition, many types of attackers exploit programming flaws such as
    1. Out-of-band data sent to an established network connection
    2. Relying mainly on global variables in programming
    3. Relying solely on user-defined functions in programming
    4. Having to alter the various data structures at the end of every run of the program
33. Which of the following is a limitation on network intrusion detection operation
    1. Operating the network at a high speed
    2. Operating the network at a low speed
    3. Having too many clients on the network
    4. Installing a firewall and a virus software on the network
34. The command ------------ is used to grant access to selective user on the web server’s configuration file on <http://www.myfile.com>
    1. < limit >

Order, allow, deny

< / limit > .my firm.com

< /directory>

* 1. < limit >

Order, allow, deny

Allow from all

< / limit > .my.firm.com

< /directory>

* 1. < directory/usr/local/http/docs >

<limit>

Order, allow, den

Deny from all

< / limit > .my firm.com

< /directory>

* 1. < limit >

Order, allow, deny

< / limit > .my firm.com/deny

< /directory>

1. Security policy considerations for a website includes

a. limiting the use of the website by visitor

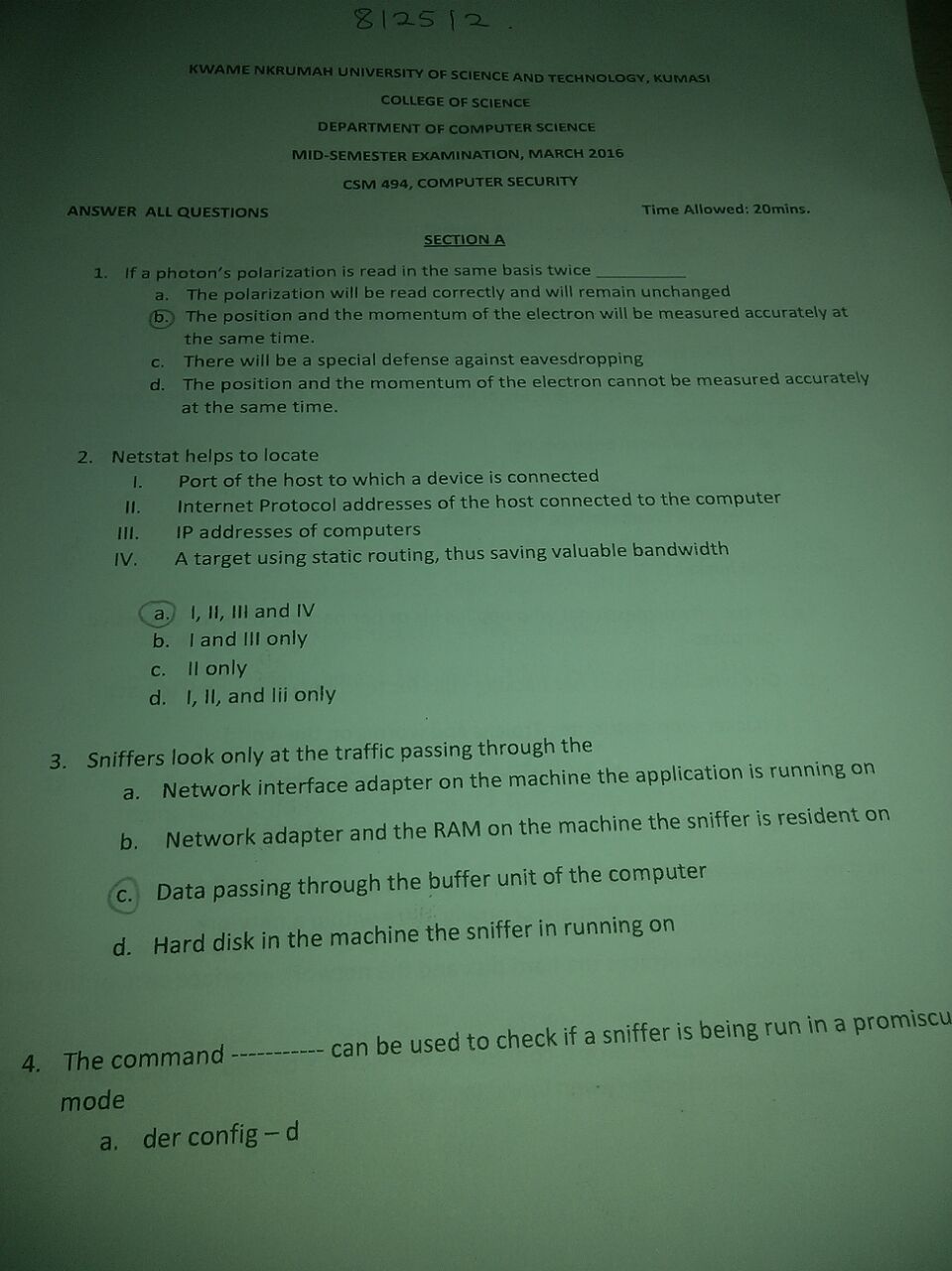
b. administering the website from the web host console

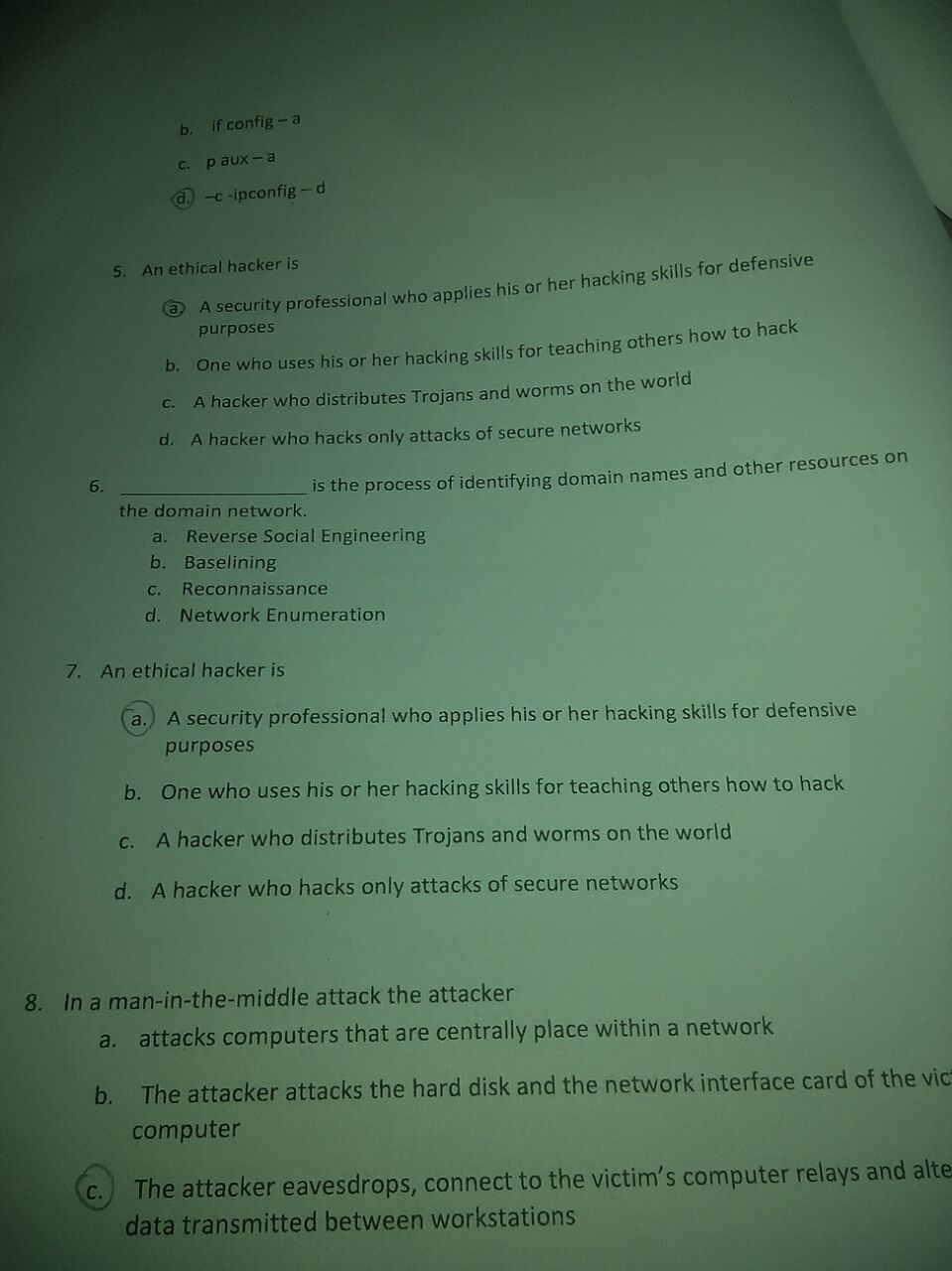
c. installing a spyware at the administrators end

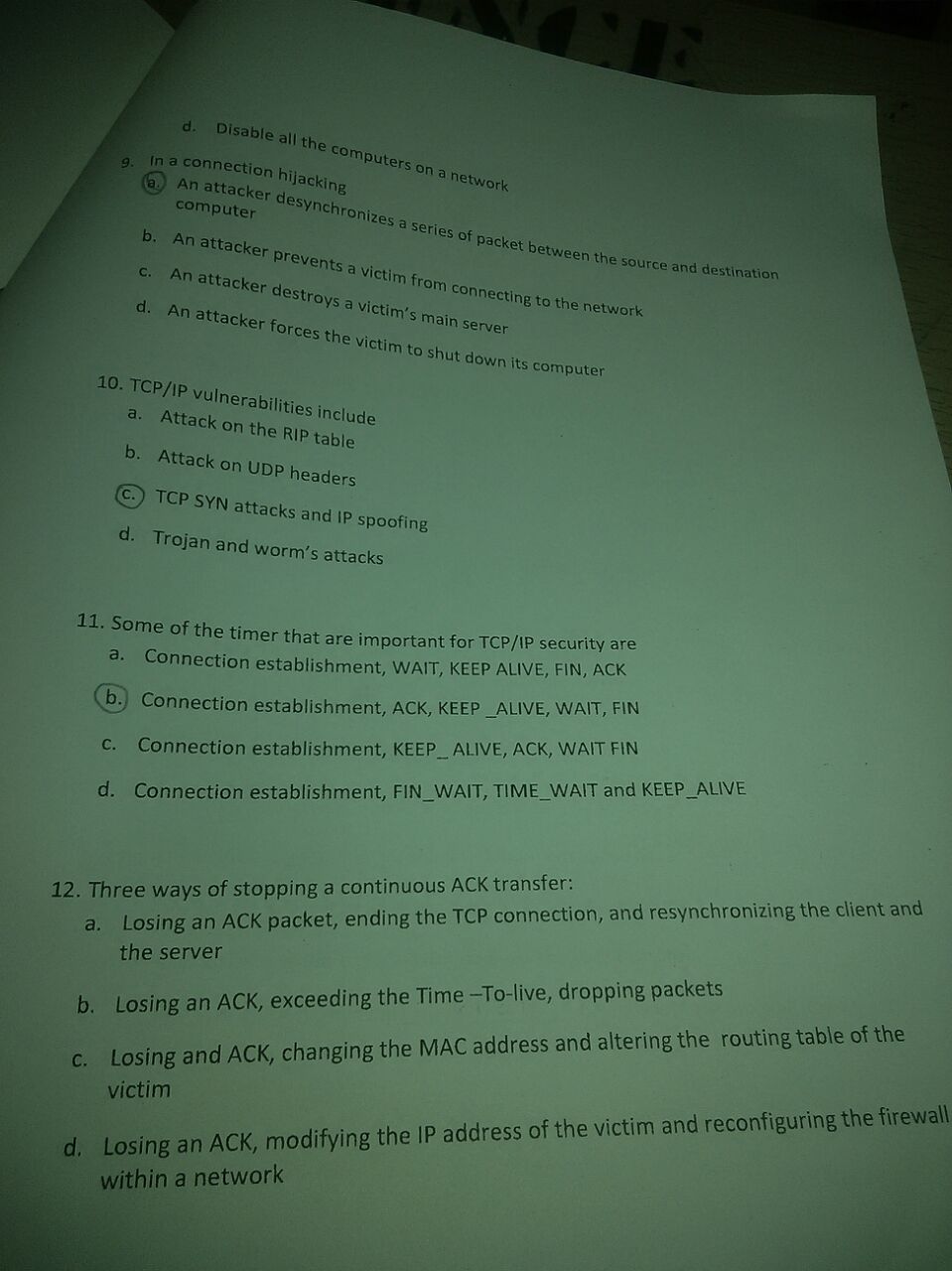
d. using a very reliable network topology

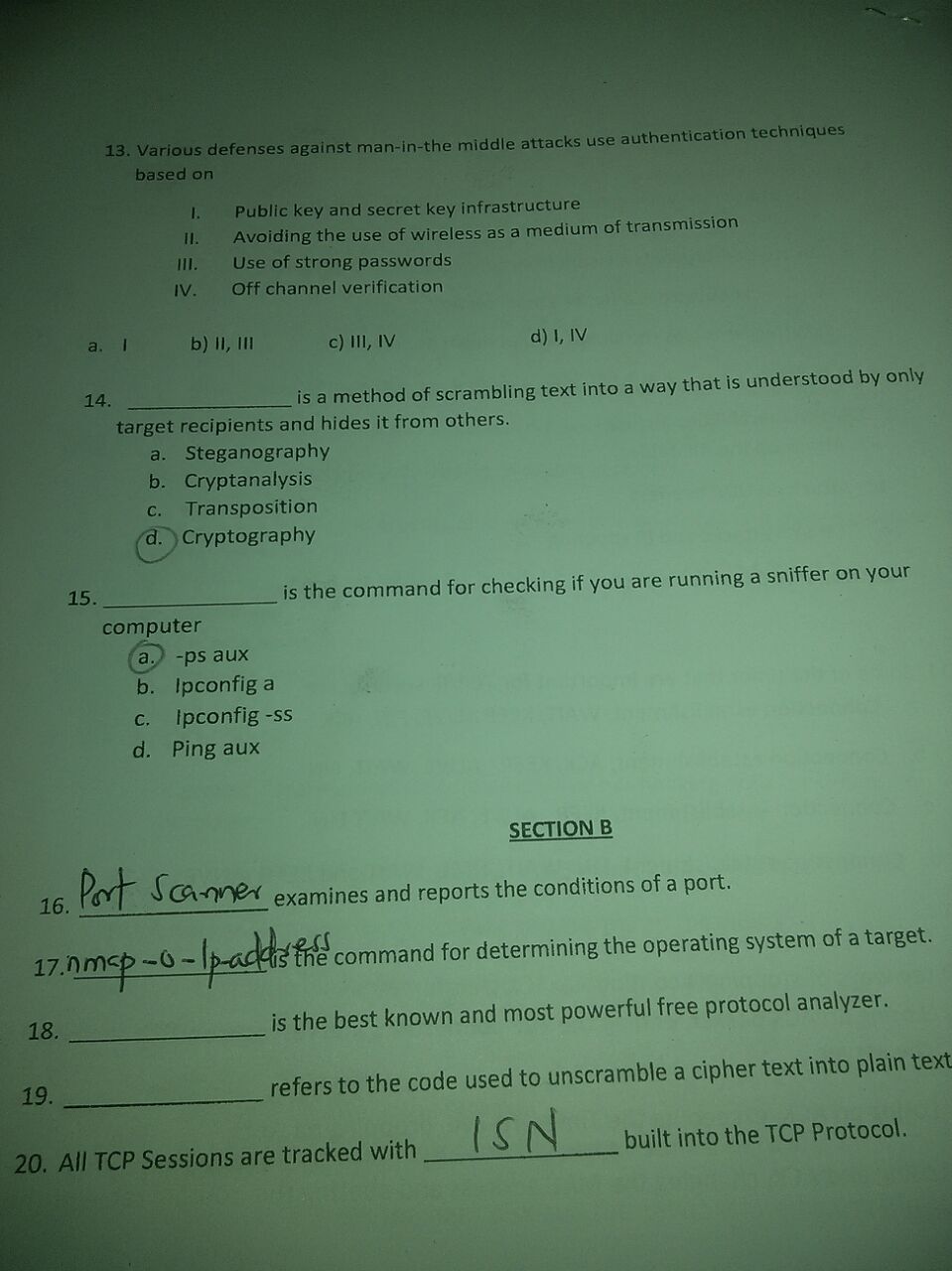
37. the very first thing you must consider on your network is the way it is connected to the internet ans also

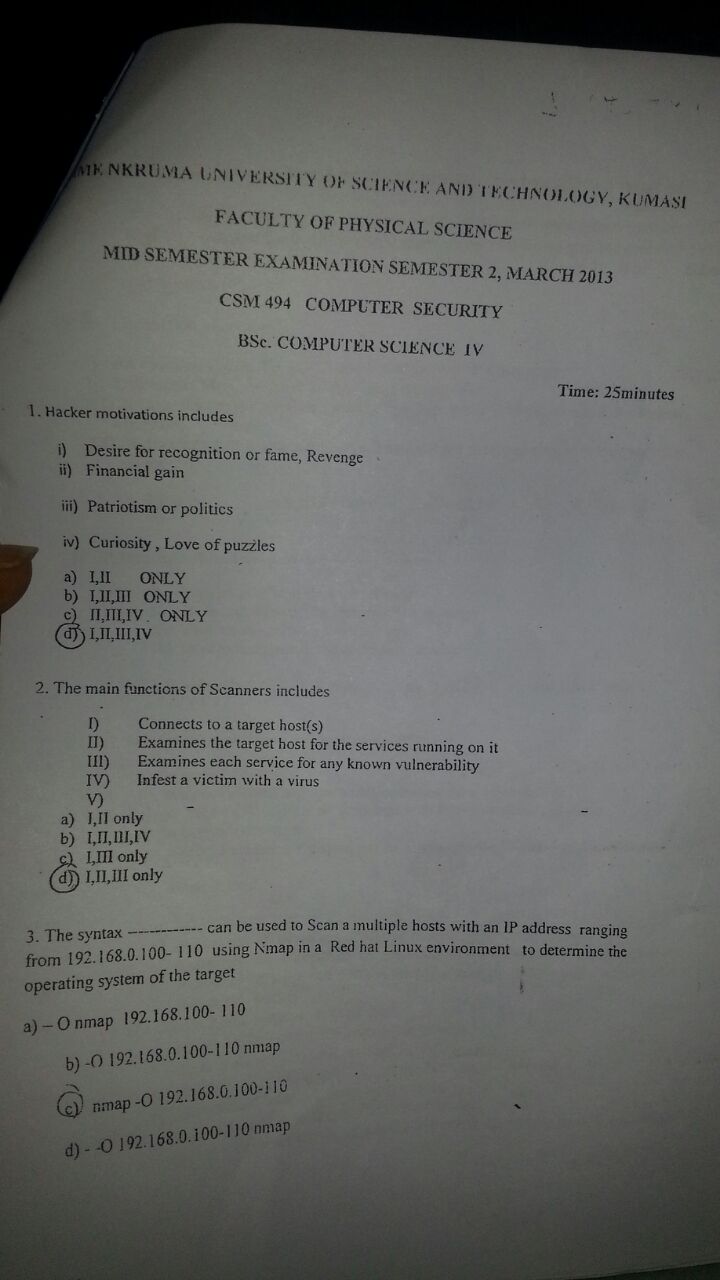
1. The operating system and the web server in use
2. The number of switches used in the network
3. The number of routers in the network
4. The strength of the proxy server in use and the type of transmission medium
5. Which of the following is a windows post-security installation method
6. Apply all hotfixes patches and updates as a number one priority and also never use passwords entry blank
7. Disable all unused icons on the desktop
8. Do not allow full access of the domain server to the clients
9. Disable any client who attempts to log-on more than the specified number of log-ons
10. A DOS attack can be prevented by
11. Filtering out frequently appearing patterns on your computer and also create and implement good security policies
12. Sending a destructive java script to the attacker computer
13. Rewriting the URL of your computer
14. Using software subversion vulnerability
15. Software subversion vulnerabilities results from the coding detects such as
16. Use of low level languages
17. Use of global variables only as the main declaration of the variables
18. Use of a buffer overflow
19. Use of only local variable
20. In a connection hijacking
21. An attacker desynchronizes a series of packet between the source and destination computer
22. An attacker prevents a victim from connecting to the network
23. An attacker destroys a victim’s main server
24. An attacker forces the victim to shut down its computer
25. In RIP (routing information protocol) attacks.
26. Attacks on RIP destroys the router of the victim’s network
27. Attacks on RIP change the destination of the data
28. Attacks on RIP disorganizes the sequence number of the packet
29. Attacks on RIP deletes the routing table of all the routers on the victims network
30. Some of the timer that are important for TCP/IP security are
31. Connection establishment, WAIT, KEEP ALIVE, FIN, ACK
32. Connection establishment, ACK, KEEP \_ALIVE, WAIT, FIN
33. Connection establishment, KEEP\_ ALIVE, ACK, WAIT FIN
34. Connection establishment, FIN\_WAIT, TIME\_WAIT and KEEP\_ALIVE
35. TCP/IP vulnerabilities include
36. Attack on the RIP table
37. Attack on UDP headers
38. TCP SYN attacks and IP spoofing
39. Trojan and worms attacks
40. IP security provides
41. Authentic addresses to victims of man-in-the middle attacks
42. Virus free packers to attackers
43. Authentication of message integrity
44. Prevents attackers from decrypting passwords of victims
45. Hackers can modify a routing table by
46. Altering Time-to-Live value in the TCP header
47. Replacing the MAC address of the victim with the hacker’s own MAC address
48. Altering the host part of the IP address of the victim’s and provide the hacker’s own IP address as the default gateway address
49. Erase all necessary records from the table and then provide the hacker’s own IP address as the default gateway address
50. Three ways of stopping a continuous ACK transfer:
51. Losing an ACK packet, ending the TCP connection, and resynchronizing the client and the server
52. Losing an ACK, exceeding the Time –To-live, dropping packets
53. Losing and ACK, changing the MAC address and altering the routing table of the victim
54. Losing an ACK, modifying the IP address of the victim and reconfiguring the firewall within a network
55. Two methods used to prevent session hijacking are
56. Encryption and storm watching
57. Firewall and anti- virus
58. Prevention of phishing and virus attacks
59. Prevention of password harvesting a network
60. To prevent a Trojan horse attack
61. You should never allow wireless connections on your network
62. You should never assign permanent IP address for clients on your network
63. Executable file formats should not be open or run unless the source of the file is known
64. Temporary files should be deleted from the hard disk.
65. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are computer that are either intentionally or unintentionally left vulnerable to an attack by crackers
66. Secure systems
67. Operating systems
68. Honey pots
69. proxies

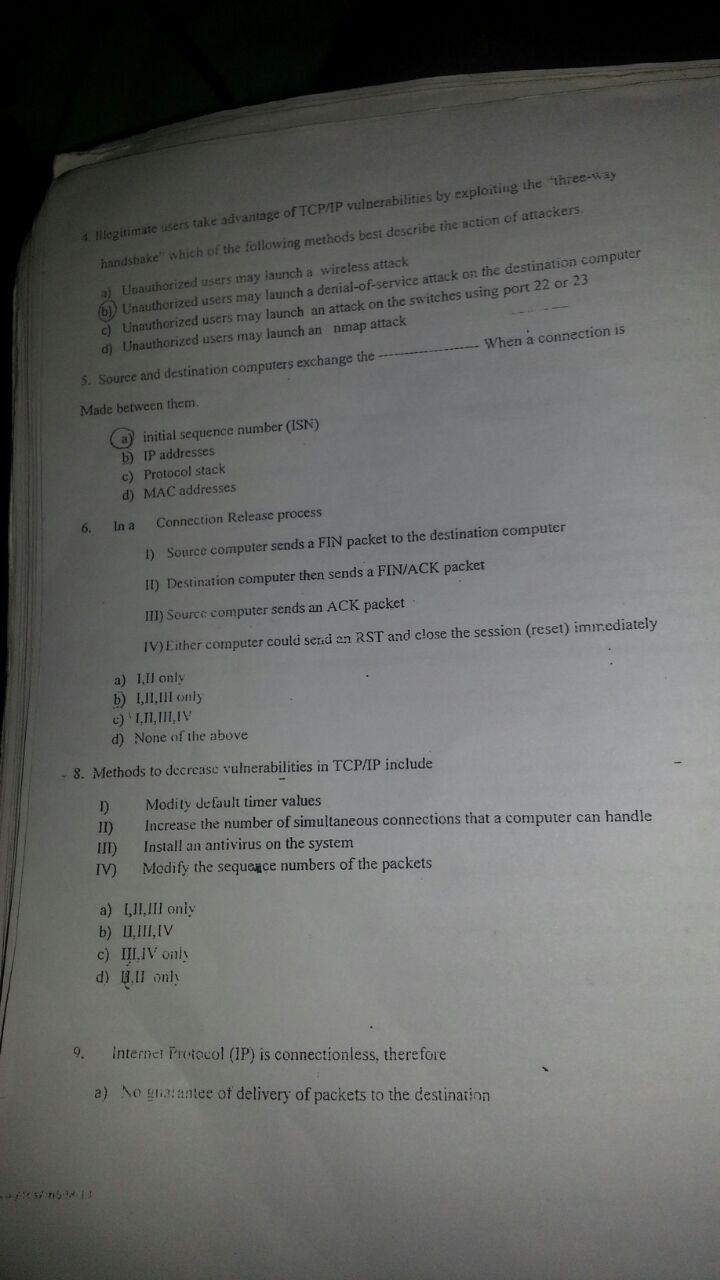


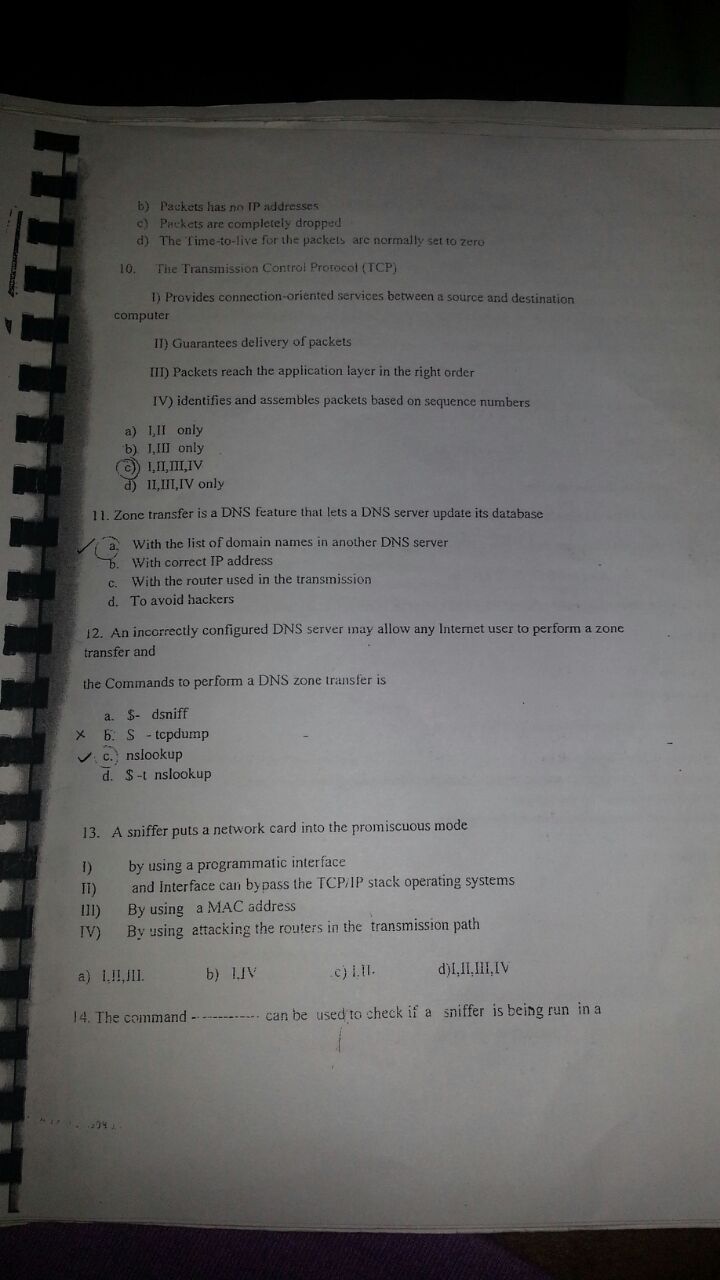


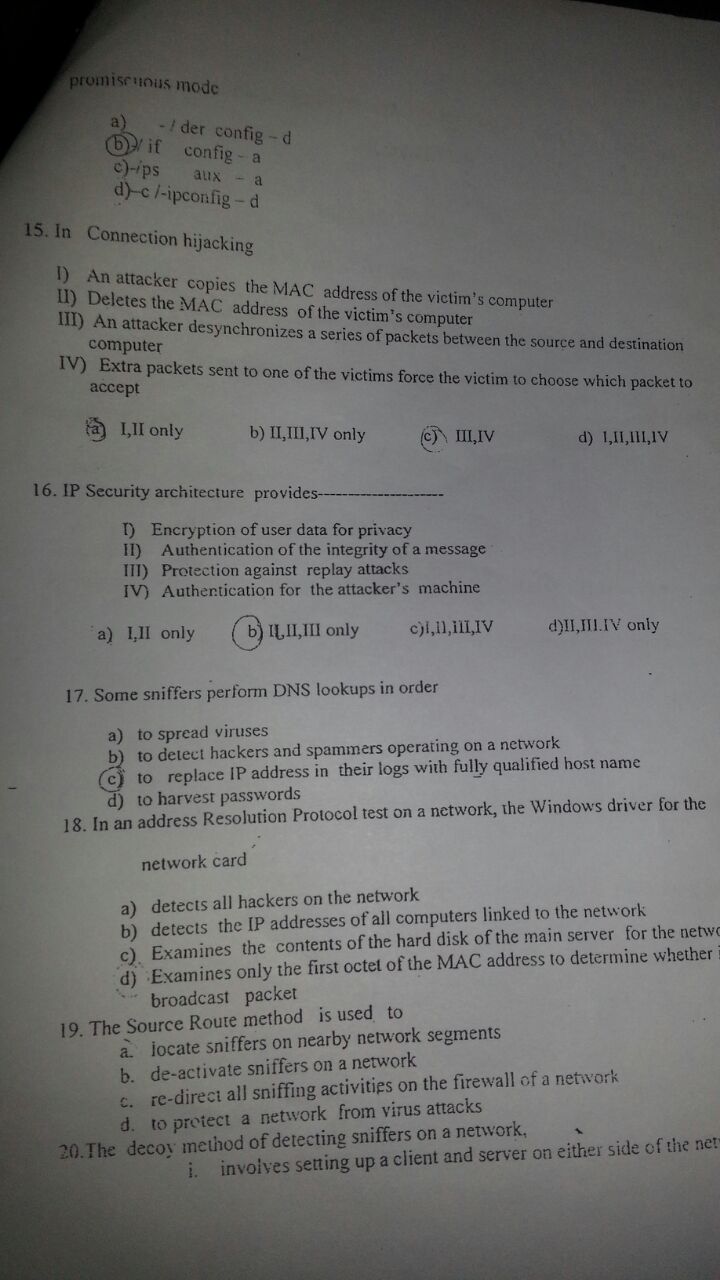












Section B Answer only one question

1a). Explain what is meant by man-in-the-middle attack and describe how it can be prevented

1b) Trojan horse payloads are almost always designed to cause harm but can also be harmless. List six types of types of Trojan horse payloads and state ten damages caused by them.

1c). differentiate between a computer virus and a computer worm and give three methods on how to protect against each of them.

1d). Describe the infection strategy of a computer virus and differentiate between a resident virus and non resident virus.

2a). Enumerate the steps involved in launching the denial-of-service (DOS) attacked.

2b). List five ways in which DoS can be perpetrated and how to service a DoS attack

2c)

1. Password crackers normally come in two flavours. Name and explain each of them

b) Give two ways each on how each of the two flavours in (a) can be defended against.

3a) Explain what is meant by email spoofing attack and state how a network can be prevented from such attack

3b) Explain how a network can be prevented from email spoofing attack

3c) In a commercial environment, the majority of software vulnerabilities results from a few known kinds of coding defects. Enumerate four of these defects.

3d). Give three ways that can be used to stop ACK transfer based on the hackers point of view.