SECTION A

1. Some sniffers perform DNS lookups in order
   a) To spread viruses
   b) To detect hackers and spammers operating on a network
   c) To replace IP address in their logs with fully quail
   d) To harvest passwords
2) The Source Route method is used to
   a) Locate sniffers on nearby network segments
   b) De-activate sniffers on a network
   c) E-direct all sniffing activities on the firewall of a network
   d) To protect a network from virus attacks
3) The decoy method of detecting sniffers on a network
   i. Involves setting up a client and server on either side of the network
   ii. The Server is configured with accounts that do not have rights or privileges
   iii. Involves configuring firewalls to attack hackers
   iv. Involves backing up all files on the main server with the network

   a) I and II b) II, III, and IV c) II and III d) I, II, III and IV
5) The command ---------- can be used to check if a sniffer is being run in a promiscuous mode
   a) -/ der config – d
   b) -/ if config – a
   c) -/ ps aux – a
   d) –c /-ip config – d
6) Motivation for hacking includes
   I. Desire for recognition or fame
   II. Desire to spread spam or virus
   III. Revenge
   IV. Intent to commit industrial, espionage

   a) I and II b)I, II, III c)II, III, IV d) I, II, III, IV
7) An ethical hacker is
   a) A security professional who applies his or her hacking skills for defensive purposes
   b) One who uses his or her hacking skills for teaching others how to hack
   c) A hacker who distributes Trojans and worms on the world
   d) A hacker who hacks only attacks of secure networks
8) Black hackers are well versed hackers who hacks websites and networks that
   a) Display valuable information
   b) Display information with a bad intent
   c) Hack with good intent
   d) Hacks sites with insufficient information
9) Sniffers are not easily detected when in operation and can be implemented from
   I. Any computer within a network
   II. At the gateway
   III. At the routers
   IV. When the link from the network to the internet is by wireless

   a) I b) I and II c)I, II and III d)I, II, III, IV
10) Sniffers look only at the traffic passing through the
   a) Network interface adaptor on the machine the application is running on
   b) Network adaptor and the RAM on the machine the sniffer is resident on
   c) Data passing through the buffer unit of the computer
   d) Hard disk in the machine the sniffer in running on
11) To spoof a trusted machine relationship, the attacker must
   I. Identify the target pair of trusted machines
   II. Anesthetize the host the attacker intends to impersonate
   III. Forge the address of the host the attacker is pretending to be
   IV. Accurately guess the correct sequence of all TCP/IP transmissions

   a) I and II only b) II, III and IV only c) III and IV d) I,II, III and IV
12) In an IP spoofing attack a tangible loss may occur when
   a) Spam or SYN flooding occur on the network under attack
   b) Valuable data is lost or duplicated

c) The network is slowed down by the attacker
d) The reputation of the victim is compromised

13) Blind spoofing is a kind of spoofing attack when the
a) Hacker is not aware of all network conditions but uses various means to gain access to the network
b) When the victim is not aware that he or she is being hacked
c) The victim's firewall cannot detect the attacker
d) Attacker can attack the victim without being detected

14) Which of the following is an example of a damage caused by Trojan horse attack?
I. Erasing or overwriting data on the affected computer
II. Re-installing itself after being disabled
III. Copying fake links which will lead to false websites or chats and other accounts based websites
IV. Rewriting the URL of the victims address
a) I and II b) II, III and IV c)I, II, III and IV d)I, II and III

15) A Trojan horse attack can be cleared by using
I. Antivirus software
II. Booting the computer from a live CD and then using an antivirus afterwards
III. Resetting jumpers on the hard disk and rebooting the whole computer
IV. Updating the firewall and testing whether the computer can be attacked
a) I and II b) II and IV c) II only d) II, III and IV

16) The best way to clean a computer which has been heavily infested by a virus is to
a) Reformat the hard disk and reinstall the operating system
b) Clean the computer with an antivirus
c) Prevent other users from using the affected files
d) Delete all unfamiliar files on the hard disk

17) Various defences against man-in-the middle attacks use authentication techniques based on
I. Public key and secret key infrastructure
II. Avoiding the use of wireless as a medium of transmission
III. Use of strong passwords
IV. Off channel verification
a) I b)II, III c) III, IV d) I, IV

18) ---------- enables closed-from solution to security that works well when only a single well-characterized property can be isolated as critical
a) Breaking the system up into smaller components
b) Zipping files
c) Using a powerful firewall
d) Using intelligent switches and routes

19) ---------- are computers that can either intentionally or unintentionally left vulnerable to attack by crackers
a) Secure systems
b) Operating systems
c) Honey pots
d) Proxies

20) In an active spoofing attack, the hacker can
I. See all the computers that reside on the victim's network
II. Hacker can hack an unsecured document on victims computer
III. Hacker can guess all sequence numbers of all TCP/IP transmissions
IV. Hacker can see both parties and perform exploits such as sniffing data, corrupting data and all the contents of a packet
a) I, II b) II, III c) I, IV d) II, III, IV

21) ARP (Address Resolution Protocol) spoofing attacks involves
I. Detecting broadcasts, faking the IP address and responding with a MAC address of the hacker's computer
II. Deleting the address of the victim's computer
III. Replacing the IP address of the victim's with the victims host address
IV. Copying the password of the victim's computer
a) I, II b) II, III, IV c) I only d) I, IV

22) In a web spoofing attack, a hacker spoofs
I. The address of the host's router and the gateway
II. The hacker redirects all information meant for the victim on to a virtual server
III. Spoofs an IP address through a website and also acquire a certificate used by a website

IV. Freezes the victims website

a) I, II b) I, II, III c) II, III, IV d) II, III

23) In a DNS spoofing on a website, the hacker changes its website's IP address to the IP address of

a) I and II b) I, I and III c) II, III, IV d) I, II, III and IV

24) An apsend which is a spoofing tool, can perform

I. SYN flood attack
II. UDP flood attack
III. Ping attack
IV. Time-to-Live attack

a) I and II b) I, II and III c) II, III, IV d)I, II, III and IV

25) Baiting as means to execute an attack relies mainly on

a) The skill of the attacker
b) The intensity of spam or flooding sent by an attacker
c) Curiosity or the greediness of the attacker
d) The efficiency of the firewall on the victims network

26) In a Quid pro quo attack, the attacker ----------

a) Helps solve a problem and in the process have the user type a command that gives the attacker access to launch a malware attack
b) Just launch a malware attack
c) The victim stuns and anesthetize the attackers computer
d) The attacker sends a bait by means of a Trojan horse and the launch a man-in-the-middle attack

27) In a man-in-the-middle attack the attacker

a) attacks computers that are centrally place within a network
b) The attacker attacks the hard disk and the network interface card of the victims computer
c) The attacker eavesdrops, connect to the victim's computer relays and alters data transmitted between workstations
d) Disable all the computers on a network

28) ---------- 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

a) Eaves dropping
b) Flooding
c) Spamming
d) Trojan horse

29) Which of the following is a type of Trojan horse payload

I. Remote accessing
II. Data destruction and security software disabler
III. Downloader
IV. Denial-of-service attack

a) I and II b)I,II and III c)II, III and IV d) I, II, III and IV

30) In an Address Resolution Protocol test, the windows driver for the network interface card

a) Detects all hackers on the system
b) Detects IP addresses of all computers attached to the network
c) Examine the contents of the hard disk of the main server for the network
d) Examines only the first octet of the MAC address

31) A firewall cannot recognize and detect internal attacks because

a) Not all firewall are reliable
b) Some hackers can by-pass a firewall
c) Firewalls can detect internal intrusive attacks if only a proxy server is present in he network
d) Firewall sit on the boundaries of networks

32) Which of the following commands can be used to detect a recently modified files on a server

a) $find/-ctime-1-print
b) $$find /-cdetect-1-detect
c) $ find/-cdisallow-1-detect
d) $deny/-ctime-1-intrusion

33) In the verification of the application layer protocols method as a means for signature recognition, many types of attackers exploit programming flaws such as

a) Out-of-band data sent to an established network connection
b) Relying mainly on global variables in programming
c) Relying solely on user-defined functions in programming

d) Having to alter the various data structures at the end of every run of the program

34) Which of the following is a limitation on network intrusion detection operation
   a) Operating the network at a high speed
   b) Operating the network at a low speed
   c) Having too many clients on the network
   d) Installing a firewall and a virus software on the network

35) The command ---------- is used to grant access to selective user on the web server's configuration file on http://www.myfile.com
   a) < limit >
      Order, allow, deny
      < / limit > .my firm.com
      < /directory>
   b) < limit >
      Order, allow, deny
      Allow from all
      < / limit > .my.firm.com
      < /directory>
   c) < directory/usr/local/http/docs >
      <limit>
      Order, allow, den
      Deny from all
      < / limit > .my firm.com
      < /directory>
   d) < limit >
      Order, allow, deny
      < / limit > .my firm.com/deny
      < /directory>

36) 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

   a. The operating system and the web server in use
   b. The number of switches used in the network
   c. The number of routers in the network
   d. The strength of the proxy server in use and the type of transmission medium

38. Which of the following is a windows post-security installation method
   a. Apply all hotfixes patches and updates as a number one priority and also never use passwords entry blank
   b. Disable all unused icons on the desktop
   c. Do not allow full access of the domain server to the clients
   d. Disable any client who attempts to log-on more than the specified number of log-ons

39. A DOS attack can be prevented by
   a. Filtering out frequently appearing patterns on your computer and also create and implement good security policies
   b. Sending a destructive java script to the attacker computer
   c. Rewriting the URL of your computer
   d. Using software subversion vulnerability

40. Software subversion vulnerabilities results from the coding detects such as
   a. Use of low level languages
   b. Use of global variables only as the main declaration of the variables
   c. Use of a buffer overflow
   d. Use of only local variable

41. In a connection hijacking

a. An attacker desynchronizes a series of packet between the source and destination computer
b. An attacker prevents a victim from connecting to the network
c. An attacker destroys a victim's main server
d. An attacker forces the victim to shut down its computer

42. In RIP (routing information protocol) attacks.
    a. Attacks on RIP destroys the router of the victim's network
    b. Attacks on RIP change the destination of the data
    c. Attacks on RIP disorganizes the sequence number of the packet
    d. Attacks on RIP deletes the routing table of all the routers on the victims network
43. Some of the timer that are important for TCP/IP security are
    a. Connection establishment, WAIT, KEEP ALIVE, FIN, ACK
    b. Connection establishment, ACK, KEEP _ALIVE, WAIT, FIN
    c. Connection establishment, KEEP_ ALIVE, ACK, WAIT FIN
    d. Connection establishment, FIN_WAIT, TIME_WAIT and KEEP_ALIVE
44. TCP/IP vulnerabilities include
    a. Attack on the RIP table
    b. Attack on UDP headers
    c. TCP SYN attacks and IP spoofing
    d. Trojan and worms attacks
45. IP security provides
    a. Authentic addresses to victims of man-in-the middle attacks
    b. Virus free packers to attackers
    c. Authentication of message integrity
    d. Prevents attackers from decrypting passwords of victims
46. Hackers can modify a routing table by
    a. Altering Time-to-Live value in the TCP header
    b. Replacing the MAC address of the victim with the hacker's own MAC address
    c. 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
    d. Erase all necessary records from the table and then provide the hacker's own IP address as the default gateway address
47. Three ways of stopping a continuous ACK transfer:
    a. Losing an ACK packet, ending the TCP connection, and resynchronizing the client and the server
    b. Losing an ACK, exceeding the Time –To-live, dropping packets
    c. Losing and ACK, changing the MAC address and altering the routing table of the victim
    d. Losing an ACK, modifying the IP address of the victim and reconfiguring the firewall within a network
48. Two methods used to prevent session hijacking are
    a. Encryption and storm watching
    b. Firewall and anti- virus
    c. Prevention of phishing and virus attacks
    d. Prevention of password harvesting a network
49. To prevent a Trojan horse attack
    a. You should never allow wireless connections on your network
    b. You should never assign permanent IP address for clients on your network
    c. Executable file formats should not be open or run unless the source of the file is known
    d. Temporary files should be deleted from the hard disk.
50. _____ are computer that are either intentionally or unintentionally left vulnerable to an attack by crackers
    a. Secure systems
    b. Operating systems
    c. Honey pots
    d. proxies

Midsem 2016

1. if a photon's polarization is read in the same basis twice_____
    a. the polarization will be read correctly and will remain unchanged
    b. The position and the momentum of the electron will be measured accurately at the same time

c. There will be a special defence against eavesdropping
d. The position and the momentum of the electron cannot be measured accurately at the same time.

2. Netstat helps to locate
   I. Port of the host to which a device is connected.
   II. Internal protocol addresses of the host connected to the computer
   III. IP addresses of computers
   IV. A target using static routing, thus saving valuable bandwidth.
      a. I, II, III and IV
      b. I and III only
      c. II only
      d. I, II, and III only
3. Sniffers look only at the traffic passing through the
   b) Network interface adaptor on the machine the application is running on
   c) Network adaptor and the RAM on the machine the sniffer is resident on
   d) Data passing through the buffer unit of the computer
   e) Hard disk in the machine the sniffer in running on
4. The command ---------- can be used to check if a sniffer is being run in a promiscuous mode
   a. -/ der config – d
   b. -/ if config – a
   c. -/ ps aux – a
   d. –c /-ip config – d
5. An ethical hacker is
   a. A security professional who applies his or her hacking skills for defensive purposes
   b. One who uses his or her hacking skills for teaching others how to hack
   c. A hacker who distributes Trojans and worms on the world
   d. A hacker who hacks only attacks of secure networks
6. _____ is the process of identifying domain names and other resources on the domain network.
   a. Reverse Social Engineering
   b. Baselining
   c. Reconnaissance
   d. Network Enumeration
7. An ethical hacker is
   a. A security professional who applies his or her hacking skills for defensive purposes
   b. One who uses his or her hacking skills for teaching others how to hack
   c. A hacker who distributes Trojans and worms on the world
   d. A hacker who hacks only attacks of secure networks
8. In a man-in-the-middle attack the attacker
   a. attacks computers that are centrally place within a network
   b. The attacker attacks the hard disk and the network interface card of the victims computer
   c. The attacker eavesdrops, connect to the victim's computer relays and alters data transmitted between workstations
   d. Disable all the computers on a network
9. In a connection hijacking
   a. An attacker desynchronizes a series of packet between the source and destination computer
   b. An attacker prevents a victim from connecting to the network
   c. An attacker destroys a victim's main server
   d. An attacker forces the victim to shut down its compute
10. TCP/IP vulnerabilities include
    a. Attack on the RIP table
    b. Attack on UDP headers
    c. TCP SYN attacks and IP spoofing
    d. Trojan and worms attacks
11. Some of the timer that are important for TCP/IP security are
    a. Connection establishment, WAIT, KEEP ALIVE, FIN, ACK
    b. Connection establishment, ACK, KEEP _ALIVE, WAIT, FIN
    c. Connection establishment, KEEP_ ALIVE, ACK, WAIT FIN
    d. Connection establishment, FIN_WAIT, TIME_WAIT and KEEP_ALIVE
12. Three ways of stopping a continuous ACK transfer:

a. Losing an ACK packet, ending the TCP connection, and resynchronizing the client and the server
b. Losing an ACK, exceeding the Time –To-live, dropping packets
c. Losing and ACK, changing the MAC address and altering the routing table of the victim
d. Losing an ACK, modifying the IP address of the victim and reconfiguring the firewall within a network

13. Various defences against man-in-the middle attacks use authentication techniques based on
    I. Public key and secret key infrastructure
    II. Avoiding the use of wireless as a medium of transmission
    III. Use of strong passwords
    IV. Off channel verification
    b)I b)II, III c) III, IV d) I, IV
14. _____ is a method of scrambling text into a way that is understood by only target recipients and hides it from others
    a. Steganography
    b. Cryptanalysis
    c. Transposition
    d. Cryptography
15. _____ is the command for checking if you are running a sniffer on your computer.
    a. –ps aux
    b. Ipconfig a
    c. Ipconfig –ss
    d. Ping aux
16. _____ examines and reports the conditions of a port.
17. _____ is the command for determining the operating system of a target.
18. _____ is the best known and most powerful free protocol analyser.
19. _____ refers to code used to unscramble a cipher text into plain text.
20. All TCP sessions are tracked with _____ built into the TCP protocol.

Midsem 2013

1. Hacker motivations includes
    i. Desire for recognition or fame, Revenge
    ii. Financial gain
    iii. Patriotism or politics
    iv. Curiousity, love of puzzles
    a. i, ii
    b. i, ii, iii
    c. ii, iii, iv
    d. i, ii, iii, iv
2. Two main functions of Scanners include
    i. Connects to a target host(s)
    ii. Examines the target host for the services running on it
    iii. Examines each service for any known vulnerability
    iv. Infest a victim with a virus
    a. i, ii
    b. i, ii, iii, iv
    c. i, iii
    d. i, ii, iii
3. The syntax _____ can be used to scan multiple hosts with an IP address ranging from 192.168.0.100 – 110 using Nmap in a Red had linux environment to determine the operating system of the target
    a. – O nmap 192.168.0.100 – 110
    b. – O 192.168.0.100 – 110 nmap
    c. nmap – O 192.168.0.100 – 110

d. – -O 192.168.0.100 – 110 nmap

4. Illegitimate users take advantage of TCP/IP vulnerabilities by exploiting the "three – way - handshake", which of the following methods best describes the action of attackers.
   a. Unauthorized users may launch a wireless attack.
   b. Unauthorized users may launch a DOS attack on the destination computer.
   c. Unauthorized users may launch an attack on the switches using port 22 or 23
   d. Unauthorized users may launch an nmap attack
5. Source and destination computers exchange the _____when a connection made between them.
   a. Initial sequence number (ISN)
   b. IP address
   c. Protocol attack
   d. MAC addresses
6. In a connection release process,
   i. Source computer sends FIN packet to the destination computer
   ii. Destination computer then sends a FIN/ACK packet
   iii. Source computer sends an ACK packet
   iv. Either computer could send an RST and close the session (reset) immediately
   a. i, ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. None of the above
7. Methods to decrease vulnerabilities in TCP/IP include
   i. Modify the default timer values
   ii. Increase the number of simultaneous connections that a computer can handle
   iii. Install an antivirus on the system
   iv. Modify the sequence numbers of the packet
   a. i, ii, iii
   b. ii, iii, iv
   c. iii, iv
   d. ii, ii
8. internet protocol (IP) is connectionless, therefore
   a. no guarantee of delivery of packets to the destination
   b. packets has no IP addresses
   c. packets are completely dropped
   d. the time – to – live for the packets are normally set to zero
9. the Transmission Control Protocol (TCP)
   i. provides connection oriented services between a source and destination computer
   ii. guarantees delivery of packets
   iii. packets reach the application layer in the right order
   iv. identifies and assembles packets based on sequence numbers
   a. i, ii
   b. i, iii
   c. i, ii, iii, iv
   d. ii, iii, iv
10. Zone transfer is a DNS feature that lets a DNS server update its database
   a. With the list of domain names in another DNS server
   b. With correct IP address
   c. With the router used in the transmission
   d. To avoid hackers
11. An incorrectly configured DNS server may allow any internet user to perform a zone transfer and the commands to perform a DNS zone transfer is
   a. $- dsniff
   b. S – tcpdump
   c. Nslookup
   d. $ - t nslookup
12. A sniffer puts a network card into the promiscuous mode
   i. By using a programmatic interface
   ii. And interface can bypass the TCP/IP stack operating systems

iii. By using a MAC address
iv. By using attacking the routers in the transmission path

a. i, ii, iii
b. i, iv
c. i, ii
d. i, ii, iii, iv

13. The command ---------- can be used to check if a sniffer is being run in a promiscuous mode
    b. -/ der config – d
    c. -/ if config – a
    d. -/ ps aux – a
    e. –c /-ip config – d
14. In a connection hijacking
    a. An attacker desynchronizes a series of packet between the source and destination computer
    b. An attacker prevents a victim from connecting to the network
    c. An attacker destroys a victim's main server
    d. An attacker forces the victim to shut down its compute
15. IP security architecture provides _____

i. Encryption of user data for privacy
ii. Authentication of the integrity of a message
iii. Protection against replay attacks
iv. Authentication for the attacker's machine

a. i, ii
b. i, ii, iii
c. i, ii, iii, iv
d. ii, iii, iv

16. Some sniffers perform DNS lookups in order
    a) To spread viruses
    b) To detect hackers and spammers operating on a network
    c) To replace IP address in their logs with fully quail
    d) To harvest passwords
17. In an Address Resolution Protocol test, the windows driver for the network interface card
    a. Detects all hackers on the system
    b. Detects IP addresses of all computers attached to the network
    c. Examine the contents of the hard disk of the main server for the network
    d. Examines only the first octet of the MAC address
18. The Source Route method is used to
    a) Locate sniffers on nearby network segments
    b) De-activate sniffers on a network
    c) E-direct all sniffing activities on the firewall of a network
    d) To protect a network from virus attacks
19. The decoy method of detecting sniffers on a network

I. Involves setting up a client and server on either side of the network
II. The Server is configured with accounts that do not have rights or privileges
III. Involves configuring firewalls to attack hackers
IV. Involves backing up all files on the main server with the network

a. I and II b) II, III, and IV c) II and III d) I, II, III and IV

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)

a) 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.