UNIT 1

1. ____ is nothing but resisting attack (1 point)

● Defence

◯ Detection

◯ Detterence

◯ None of the above

2. Three D's of the security are_____ (1 point)

◯ Defence , Dynamic, Does

◯ Detect, Display, Dynamic

● Defence ,Detection,Deterrence

◯ None of the above

3. _____model has multiple layer of security (1 point)

● Onion

◯ Lolipop

◯ Both

◯ None of the above

4. _____ is a standalone computer program that replicate itself in order to spread itself. (1 point)

● Worms

◯ Trojans

◯ Virus

◯ None of the above

5. DoS stands for (1 point)

◯ Data of security

● Denial of service

◯ Denial on service

◯ None of the above

6. _____ means that the data has not been altered in an unauthorized way (1 point)

◯ Confidentiality

● Integrity

◯ Availability

◯ None of the above

7. _____attack attempts to learn or make use of information from the system but does not affect resources.

(1 point)

◯ Active Attack

● passive attack

◯ User

◯ None of the above

8. _____ is a measure how easily data and software can be transferred from one organization to other organization

(1 point)

◯ Carriers

◯ Transport

● Portability

◯ None of the above

9. _____is the process of identifying presence of some malicious activity which is concealed

(1 point)

● Detection

◯ Detterence

◯ Defence

◯ None of the above

10. _____is a path or tool used by the hacker to attack the sysytem (1 point)

◯ Threat

● Threat Vector

◯ User

◯ None of the above

11. _____ means that only the authorized individual or system can view sensitive information

(1 point)

● Confidentiality

◯ Integrity

◯ Availability

◯ None of the above

12. _____model has only one layer of security (1 point)

◯ Onion

● Lolipop

◯ Both

◯ None of the above

13. _____refers to the ability of the organization that allows it to respond rapidly to the changes in the external and internal environment

(1 point)

● Business Agility

◯ Portability

◯ Cost Reduction

◯ Security Methodology

14. _____is a malware that is disguised as legitimate software and which can be used to gain backdoor access to users computer

(1 point)

◯ Worms

● Trojan

◯ Virus

◯ None of the above

15. _____ is a self replicating program that uses other host files or code to replicate (1 point)

◯ Worms

◯ Trojans

● Virus

◯ None of the above

16. _____attack attempts to modify the system resources or affect their operations (1 point)

● Active Attack

◯ passive attack

◯ User

◯ None of the above

17. Every IP address is of _____bits (1 point)

◯ 40

● 32

◯ 48

◯ None of the above

18. MAC stands for _____ (1 point)

● Media access control

◯ Machine access control

◯ Man access control

◯ None of the above

19. _____is an effective method of reducing frequency of security compromises ,and thereby total loss due to security incidents

(1 point)

◯ Detection

● Detterence

◯ Defence

◯ None of the above

20. _____is an an important assets for any company or organization (1 point)

◯ Employees

● Information

◯ Salary

◯ None of the above

UNIT 2

1. The process of converting encrypted form of text back to its original form is called (1 point)

◯ Encryption

● Decryption

◯ Cryptosystem

2. _____is a security mechanism used to determine user previledges or access levels related to system resources

(1 point)

◯ Authentication

● Authorization

◯ Both the above

3. Biometrics is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

4. _____factor authentication involves two level authentication (1 point)

◯ MFA

◯ SFA

● Two factor authentication

5. Local storage and comparison is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

6. User rights is a type of _____ (1 point)

◯ Authentication

● Authorization

◯ Both the above

7. In Public key cryptography encryption is done using (1 point)

◯ Senders public key

● Receivers public key

◯ Senders private key

8. _____ cryptography uses the same key for encryption and decryption (1 point)

● Symmetric key cryptography

◯ Asymmetric key cryptography

◯ PKI

9. In _____cryptography system the key is shared to receiver before data transform (1 point)

◯ Asymmetric key cryptography

● Symmetric key cryptography

◯ PKI

10. RBAC is a type of _____ (1 point)

◯ Authentication

● Authorization

◯ Both the above

11. Use of OTP is _____type of authentication (1 point)

◯ MFA

◯ SFA

● Two factor authentication

12. _____ cryptography uses the different key for encryption and decryption (1 point)

● Asymmetric key cryptography

◯ Symmetric key cryptography

◯ PKI

13. _____ is a method of encoding a message into a non readable format (1 point)

◯ Conversion

● Encryption

◯ Decryption

14. Kerberos is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

15. The encrypted form of text is called as _____ (1 point)

◯ Encryption

◯ Decryption

● Cipher text

16. In Public key cryptography decryption is done using (1 point)

● Receivers private key

◯ Receivers public key

◯ Senders private key

17. Username and password is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

18. One time password system is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

19. _____key is known to all (1 point)

◯ Private

● Public

◯ Both

20. File access permission is a type of _____ (1 point)

◯ Authentication

● Authorization

◯ Both the above

21. Central storage and comparison is a method of _____ (1 point)

● Authentication

◯ Authorization

◯ Both the above

22. _____ is the process of determining who is the user (1 point)

● Authentication

◯ Authorization

◯ Identification

23. In Public key cryptography decryption is done using (1 point)

● Receivers private key

◯ Receivers public key

◯ Senders private key

24. ACL stands for _____ (1 point)

◯ Access control line

◯ Access counter list

● Access control list

25. ACL is a type of _____ (1 point)

◯ Authentication

● Authorization

◯ Both the above

26. Username and password is _____ type of authentication (1 point)

◯ MFA

● SFA

◯ Two factor authentication

27. System used for encryption and decryption is known as_____ (1 point)

◯ Encry decry system

◯ Transformation

● Cryptosystem

21. _____ comparers the desired state of security program with the actual current state and identifies the difference

(1 point)

◯ Risk Analysis

● Gap Analysis

◯ Both

◯ None of the above

22. _____is an attack where an application inject a specially crafted packet on to the network repeatedly

(1 point)

◯ ARP Posoning

● MAC Flooding

◯ DHCP poisoning

◯ None of the above

23. The act of capturing data packets across the computer network by an unauthorized third party destined for computers other than their own is called _____

(1 point)

◯ Attack

● Packet sniffing

◯ Theft

◯ None of the above

24. _____model was an open model (1 point)

◯ Government model

● Academic model

◯ Both Gov and academic

◯ None of the above

25. _____ means that the dat a should be available as an when needed (1 point)

◯ Confidentiality

◯ Integrity

● Availability

◯ None of the above

UNIT 3

1. _____device forward the packet received at one port to all other port without storing

(1 point)

◯ Switch

◯ Router

● Hub

2. ____ layer is responsible for host to host delivery (1 point)

● Network

◯ Data link layer

◯ Transport layer

3. _____ is also private network controlled by organization and can be used for providing application access to trusted external parties such as supplier, vendors,partners and customers

(1 point)

◯ Internet

◯ Intranet

● Extranet

4. It is possible to prevent direct connection between external and internal users via _____

(1 point)

◯ Firewall

● Proxy services

◯ ACL

5. _____ is a hardware, software or combination of both that monitors and filters the traffic that coming or going out the network

(1 point)

● Firewall

◯ IPS

◯ ACL

6. IPV6 addresses are _____bit in a size (1 point)

◯ 48

● 128

◯ 16

7. To send traffic ,sending device must have destination device _____ address (1 point)

◯ IP address

◯ MAC

● Both the above

8. _____layer is concern with the syntax and symantics of the information (1 point)

◯ Application layer

● Presentation layer

◯ Session layer

9. _____are the set of changes to a computer designed to update,fix or improve it (1 point)

● Patches

◯ Protocol

◯ Standard

10. In Cisco H. Model _____layer aggregates traffic from all nodes and uplinks from the access layer and provide policy based connectivity.

(1 point)

◯ Access layer

◯ Core layer

● Distribution layer

11. _____layer is responsible for delivery of message from one process to other (1 point)

◯ Physical layer

◯ Data link layer

● Transport layer

12. _____ is a private network of an organization which is accessible only to the members of the organization

(1 point)

◯ Internet

● Intranet

◯ Extranet

13. _____ provide the mechanism to reporting TCP/IP communication problems (1 point)

◯ ARP

◯ RARP

● ICMP

14. MAC addresses are ____ bit hexadecimal colon separated numbers assigned to NIC by the manufacturer

(1 point)

● 48

◯ 32

◯ 16

15. High availability ,security, quality of service and IP multicasting are the features of

_____layer

(1 point)

● Access layer

◯ Core layer

◯ Distribution layer

16. An acceptable level of information systems risk depends on the individual organization and its ability to tolerate risk

(1 point)

● True

◯ False

17. _____device is used to connect two different network (1 point)

◯ Switch

● Router

◯ Hub

18. _____device forward the received packet to only one port for its correct destination (1 point)

● Switch

◯ Router

◯ Hub

19. In Cisco H. Model _____layer forms the network backbone and it is focused on moving data as fast as possible between distribution layers

(1 point)

◯ Access layer

● Core layer

◯ Distribution layer

20. _____ is a hardware, software or combination of both that monitors and filters the traffic that coming or going out the network

(1 point)

● Firewall

◯ IPS

◯ ACL

UNIT 4

1. TEM stands for _____ (1 point)

◯ Telephone expert management

◯ telecommunication expense manager

● Telecom expense management

2. _____is a telephone services over Internet (1 point)

◯ Voice Internet

◯ VIP

● VoIP

3. _____consist of an agent on a host that identifies and intrusion by analysing system calls, application logs,etc

(1 point)

◯ SIDS

◯ NIDS

● HIDS

4. _____ identifies packets when it going through TCP/IP stack (1 point)

● SIDS

◯ NIDS

◯ HIDS

5. _____ type of security classification of computer system uses formal design specification and variation techniques

(1 point)

● Type A

◯ Type B

◯ Type C

6. _____method of detection uses signatures ,which are attack patterns that are

preconfigured and predetermined

(1 point)

◯ Statistical anomly based detection

◯ Stateful protocol analysis decison

● signature based detection

7. _____ method identifies deviations of protocol states by comparing observed events with predetermined profile of generally accepted definition of begin activity

(1 point)

● Stateful protocol analysis decison

◯ signature based detection

◯ Click Statistical anomly based detection add a new answer choice

8. _____is a telephone system within an enterprise that switches call between enterprise users on local lines while allowing all users to share certain no. of external phone lines

(1 point)

◯ Public branch exchange

● PBX

◯ phone bank exchange

9. SAMM stands for _____ (1 point)

◯ Software as a multilayer module

● Software assurance maturity model

◯ Software assurance model maturity

10. HIDS stands for (1 point)

Host based intrusion detection system

11. SIEM stands for _____ (1 point)

◯ security information protocol

◯ Secure information and event management

● Security information and event management

12. _____is an independent platform that identifies intrusion by examining network traffic and monitors multiple host

(1 point)

◯ SIDS

● NIDS

◯ HIDS

13. As per U.S Department of users trusted computer systems evaluation criteria there are _____ security classifications in computer system

(1 point)

◯ 1

◯ 3

● 4

14. IPS stands for _____ (1 point)

◯ intrusion protection system

● intrusion prevention sysytem

◯ Intrusion private system

15. IDS stands for (1 point)

intrusion detection system

16. NIDS stands for (1 point)

Network intrusion decision system

17. _____is a open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risk facing the organizations

(1 point)

● SAMM

◯ PBX

◯ VOiP

18. _____is a term used to define an approach to managing all telephone service expense such as voice ,data,etc

(1 point)

● TEM

◯ PBX

◯ VOiP

19. SIDS stands for (1 point)

Stack based intrusion detection system

20. _____attack is an attempt to make a system inaccessible to its legitimate users (1 point)

◯ passive attack

● DDoS

◯ Active attack

UNIT 5

1. _____ virtual machine support the host computers physical resources between

multiple virtual machines,each running with its own copy of the operating system

(1 point)

◯ Process virtual machine

● system virtual machine

◯ none of the above

2. _____ phase if SDL consist of activities that occur prior to writing code (1 point)

◯ Requirment

● Design

◯ Coding

3. _____provides us means by which we can access the applications as utilities over

the Internet

(1 point)

◯ virtual machine

◯ system virtual machine

● Cloud computing

4. Yahoo messenger is not a example of thick client (1 point)

◯ True

● False

5. Two tier thick client application uses user computer and _____ (1 point)

◯ Local computer

● Server

◯ Database

6. _____of the following service provides companies with computing resources including server, networking,storage and data center space etc

(1 point)

● IaaS

◯ SaaS

◯ PaaS

7. SDL stands for_____ (1 point)

◯ Software development life cycle

● Secure development life cycle

◯ standard life cycle

8. Three tier thick client application uses user computer ,application server and _____ (1 point)

◯ Local computer

◯ Remote Computer

● Database

9. Full form of SaaS (1 point)

Software as a service

10. Microsoft outlook is a example of thick client (1 point)

● True

◯ False

11. Depending on use and level of dependencies virtual machines can be devided into _____ categories

(1 point)

◯ 1

● 2

◯ 3

12. _____of the following service provides a cloud based environment with everything required to support the complete life cycle of building and delivering cloud based application without the cost and complexity of buying and managing the underlying hardware and software,provisios etc

(1 point)

◯ IaaS

◯ SaaS

● PaaS

13. _____is designed to provide platform independent programming environment that makes the information of the underlying hardware or OS and allows program execution to take place in the same way on the given platform

(1 point)

● Process virtual machine

◯ system virtual machine

◯ none of the above

14. Full form of PaaS (1 point)

Platform as a service

15. Yahoo.com is not a example of thin client (1 point)

◯ True

● False

16. _____ clients are heavy applications which involve normally the installation of application on the user computer

(1 point)

● thick client

◯ thin client

◯ None of the above

17. Full form of IaaS (1 point)

Infrastructure as a service

18. Creating computer within a computer is known as _____ (1 point)

● Virtual Machine

◯ Nested Computer

◯ Computer in Computer

19. _____ client applications are web based applications which can be accessed on the Internet using a browser

(1 point)

◯ thick client

● thin client

◯ None of the above

20. Write any one recommendation for Application-Focused security (1 point)

Treat infrastructure as unknown and insecure

21. _____ is a computer file typically called an image,which behave like an actual computer

(1 point)

● Virtual Machine

◯ computer image

◯ Computer in Computer

22. Google.com is a example of thin client (1 point)

● True

◯ False

Security in Computing

Unit 1

1. is one of the most important assets a company possesses.

a) Employees

b) Resources

c) Information

d) Money

Ans: Information

2. Confidential information is available to external audiences only for business-related purposes and only after entering

a or equivalent obligation of confidentiality.

a) Nondemocratic Agreement (NDA)

b) Nondisclosure Agreement (NDA)

c) National Democratic Alliance (NDA)

d) Nondisclosure Alliance (NDA)

Ans: Nondisclosure Agreement (NDA)

3. Originally, the academic security model was and the government security model was .

a) closed and locked, wide open

b) wide locked, open and closed

c) wide and open, wide and closed

d) wide open, closed and locked

Ans: wide open, closed and locked

4. A approach doesn't work when you need to allow thousands or millions of people to have access to

the services on your network.

a) closed-door

b) open-door

c) wide-door

d) locked-door

Ans: closed door

5. An approach doesn't work when you need to protect the privacy of each individual who interacts with

the services on your network.

a) closed-door

b) open-door

c) wide-door

d) locked-door

Ans: open-door

6. As more companies started doing business on the Internet, concepts such as were developed

to provide business services over the Internet.

a) Software-as-a-Service (SaaS)

b) Virtual private networks (VPNs)

c) Personally identifiable information (PII)

d) Storage as a Service (SaaS)

Ans: Software-as-a-Service (SaaS)

7. What can result in service outages during which customers cannot make purchases and the company cannot transact

business?

a) virus outbreak

b) web site outage

c) denial of service (DoS) attack

d) All of the above

e) None of the above

Ans: All of the above

8. means that software and data can be used on multiple platforms or can be transferred/transmitted

within an organization, to a customer, or to a business partner.

a) Portability

b) Accessibility

c) Authority

d) Sharing

Ans: Portability

9. is concerned with protecting information in all its forms, whether written, spoken, electronic,

graphical, or using other methods of communication.

a) Software Security

b) Information Security

c) Network Security

d) Storage Security

Ans: Information security

10. is concerned with protecting data, hardware, and software on a computer network.

a) Software Security

b) Information Security

c) Network Security

d) Storage Security

Ans: Network security

11. The three Ds of security stand for:

a) Defense, dedication, and deterrence

b) Defense, detection, and discipline

c) Defense, detection, and deterrence

d) Defense, detection, and diligence

Ans: defense, detection, and deterrence

12. Without adequate a security breach may go unnoticed for hours, days, or even forever.

a) Detection

b) Deterrence

c) Defense

d) All of the above

Ans: Detection

13. The 3 aspects of Security are:

a) Defense, dedication, and deterrence

b) Defense, detection, and discipline

c) Defense, detection, and deterrence

d) Defense, detection, and diligence

Ans: defense, detection, and deterrence

14. provides a defensible approach to building the program.

a) Security program

b) Security framework

c) Planning

d) Security initiatives

Ans: Security framework

15. A security program defines the purpose, scope, and responsibilities of the security organization and

gives formal authority for the program.

a) Charter

b) Memo

c) Document

d) File

Ans: Charter

16. The provides a framework for the security effort.

a) Security program

b) Security framework

c) Security policy

d) Security initiatives

Ans: Security framework

17. change with each version of software and hardware, as features are added and functionality changes,

and they are different for each manufacturer.

a) Standards

b) Rules

c) Application

d) Files

Ans: Standards

18. Guidelines for the use of software, computer systems, and networks should be clearly documented for the sake of

the people who use these technologies.

a) Standards

b) Rules

c) Guidelines

d) Security

Ans: Guidelines

19. provides a perspective on current risks to the organization’s assets.

a) Risk Analysis

b) Planning

c) Guidelines

d) Security

Ans: Risk Analysis

20. compares the desired state of the security program with the actual current state and identifies the differences.

a) Risk Analysis

b) Security Analysis

c) Comparison Analysis

d) Gap Analysis

Ans: Gap Analysis

21. is a plan of action for how to implement the security remediation plans.

a) Charter

b) Outline

c) Roadmap

d) Layout

Ans: Roadmap

22. The documents how security technologies are implemented, at a relatively high level.

a) Charter

b) Security architecture

c) Roadmap

d) Layout

Ans: security architecture

23. The actions that should be taken when a security event occurs are defined in? the incident response plan.

a) Charter

b) Security architecture

c) Roadmap

d) Incident response plan

Ans: Incident response plan

24. is the process of defense, is the process of insurance, and is deciding that the risk

does not require any action.

a) Planning, transference, acceptance

b) Planning, mitigation, acceptance

c) Transference, mitigation, acceptance

d) Mitigation, transference, acceptance

Ans: Mitigation, transference, acceptance

25. is a term used to describe where a threat originates and the path it takes to reach a target.

a) Threat vector

b) Origin vector

c) Target vector

d) Trojan vector

Ans: Threat vector

26. refers to a Trojan program planted by an unsuspecting employee who runs a program provided by a trusted friend from a storage device like a disk or USB stick, that plants a back door inside the network.

a) Threat exploit

b) Friend exploit

c) Girlfriend exploit

d) Trusted exploit

Ans: Girlfriend exploit

27. Which are the generally recognized variants of malicious mobile code?

a) Viruses

b) Worms

c) Trojans

d) a and b

e) a, b and c

Ans: a, b and c

28. is a self-replicating program that uses other host files or code to replicate.

a) Virus

b) Worm

c) Trojan

d) None of the above

Ans: Virus

29. If the virus executes, does its damage, and terminates until the next time it is executed, it is known as?

a) Temporary virus

b) Resident virus

c) Nonresident virus

d) Stealth virus

Ans: Nonresident virus

30. If the virus stays in memory after it is executed, it is called?

a) Permanent virus

b) Memory-resident virus

c) Memory Nonresident virus

d) None of the above

Ans: Memory-resident virus

31. Which viruses insert themselves as part of the operating system or application and can manipulate any file that is

executed, copied, moved, or listed?

a) Permanent viruses

b) Memory-resident viruses

c) Memory Nonresident viruses

d) None of the above

Ans: Memory-resident virus

32. If the virus overwrites the host code with its own code, effectively destroying much of the original contents, it is

called?

a) Overwriting virus

b) Stealth virus

c) Nonresident virus

d) Parasitic virus

Ans: Overwriting virus

33. If the virus inserts itself into the host code, moving the original code around so the host programming still remains

and is executed after the virus code, the virus is called?

a) Overwriting virus

b) Stealth virus

c) Prepending virus

d) Parasitic virus

Ans: Parasitic virus

34. Viruses that copy themselves to the beginning of the file are called? prepending viruses

a) Overwriting virus

b) Appending virus

c) Prepending virus

d) Parasitic virus

Ans: Prepending virus

35. Viruses placing themselves at the end of a file are called?

a) Overwriting virus

b) Appending virus

c) Prepending virus

d) Parasitic virus

Ans: Appending virus

36. Viruses appearing in the middle of a host file are labeled? mid-infecting viruses.

a) Mid-infecting viruses

b) Appending viruses

c) Prepending viruses

d) Parasitic viruses

Ans: Mid-infecting viruses

37. Who works by posing as legitimate programs that are activated by an unsuspecting user?

a) Virus

b) Worm

c) Trojan

d) None of the above

Ans: Trojan

38. Which type of Trojans infect a host and wait for their originating attacker's commands telling them to attack other hosts.

a) Directed Action Trojans

b) Zombie Trojans

c) Remote Access Trojans

d) None of the above

Ans: Zombie Trojans

39. CIA stands for?

a) Confidentiality, Integrity, and Availability

b) Confidentiality, Integrity, and Accessibility

c) Confirmity, Integrity, and Accessibility

d) Confidentiality, Integrity, and Authority

Ans: Confidentiality, Integrity, and Availability

40. refers to the restriction of access to data only to those who are authorized to use it.

a) Confidentiality

b) Authority

c) Accessibility

d) None of the above

Ans: Confidentiality

41.Onion model is also known as:

a) Perimeter Security

b) Defense in depth

c) Both of the above

d) None of the above

Ans: Defense in depth

1) What control can be used to help mitigate identified risks to acceptable levels?
   a. Authentication b. Authorization c. Decryption d. Management

   Ans: Authentication

2) Which one is the key network design strategy?
   a. Performance b. Cost of Security c. Routing d. Encryption

   Ans: Cost of Security

3) Which technologies may be considered by the design team to prevent one application from consuming too much of bandwidth?

   a. Electronic Security Perimeter(ESP)

   b. Software-as-a-Service(SaaS)

   c. Public Switched Telephone Network(PSTN)

   d. Quality of Service(QoS)

   Ans: Quality of Service

4) How many layers does Cisco Internetworking model has?

   a. Three b. Four c. Two d. One

   Ans: Three

5) What is Core layer's primary focus?

a. Filtering b. Encryption c. Performance d. Compressing

Ans: Performance

6) _____ layer is composed of the user networking connections.

a. Access layer b. Core layer c. Distribution layer d. Firewall

Ans: Access layer

7) Which architecturing approach offers higher performance and lower cost but also brings special security considerations into play.

a. Single-tier b. Three-tier c. Multi-tier d. collapsed two-tier

Ans: collapsed two-tier

8) What helps us to understand how to use routers and switches to increase the security of the network?

a. Security Network Design

b. Wireless Network Security

c. Network Device Security

d. Firewalls

Ans: Security Network Design

9) The dominant internetworking protocol in use today is known as _____.

a. TCP/IP b. HTTPS c. FTP d. UTM

Ans: TCP/IP

10) MAC addresses are ____ bit hexadecimal numbers that are uniquely assigned to each hardware network interface by the manufacturer.

a. 8 b. 24 c. 48 d. 64

Ans: 48

11) IPv4 addresses are ___ bits.

a. 8 b. 32 c. 64 d. 128

Ans: 32

12) IPv6 addresses are ____ bits.

a. 128 b. 32 c. 24 d. 64

Ans: 128

13) The host uses the _____ , which functions by sending a broadcast message to the network that basically says, " Who has 192.168.2.10, tell 192.168.2.15".

a. Network Interface Card(NIC)

b. Domain Name Server(DNS)

c. Address Resolution Protocol (ARP)

d. Open System Connection (OSI)

Ans: Address Resolution Protocol (ARP)

14) How many layers does OSI model contain?

a. Five b. Six c. Four d. Seven

Ans: seven

15) _____ an OSI-model layer is used to convert application data into acceptable and compatible formats for transmission. At this layer, data is encrypted and encoded and encrypted.

a. Presentation b. Application c. Transport d. Network

Ans: Presentation

16) Which is most well-known application-layer protocols in use today?

a. TCP/IP b. UDP c. HTTP d. FTP

Ans: HTTP

17) Which layer provides mechanism for two host to maintain network connections .

a. Data-link layer b. Session layer c. Physical layer d. Transport layer

Ans: Session layer

18) Which layer provides unique address to every host on the network .

a. Application layer b. Physical layer c. Transport layer d. Network layer

Ans: Network layer

19) _____ layer is composed of two sub layers : Media Access Control (MAC) and Logical Link Control (LLC).

a. Data-link b. Transport c. Application d. Physical

Ans: Data-link

20) As the size of the network increases, the distance and time a packet is in transmit over the network also _____ , making collision more likely.

a. Increases b. Decreases c. All of the above d. None of the above

Ans: Increases

21) Routers and switches operate at layers ___ and ___ respectively.

a. Two and three b. Three and Two c. One and Two d. Three and Four.

Ans: Three and Two

22) In which two ways routers learn the locations of various networks ?

a. Dynamically and Statically

b. Dynamically and Manually

c. All of the above

d. None of the above

Ans: Dynamically and Manually

23) What are the two main types of layer three (Routing) protocols?

a. Dynamic and static

b. Distance-vector and Link-state

c. Manual and Static

d. None of the above

Ans: Distance-vector and Link-state

24) Which one of the following is a network hardening method?

a. Remote Access Considerations

b. Network Modelling

c. The cost of Security

d. Patching

Ans: Patching

25) What can be configured to permit or deny TCP, UDP, or other types of traffic based on the source or the destination address.

a. Disabling Unused Services

b. Access Control Lists

c. Patching

d. Switch Security Practices

Ans: Access Control List

26) Which one of the following comes under Disabling Unused Services?

a. Access Control Lists

b. Administrative Practises

c. Proxy ARP

d. Patching

Ans: Proxy ARP

27) _____ provides a mechanism for reporting TCP/IP communication problems, as well as utilities for testing IP layer connectivity.

a. Simple Network Management Protocol (SNMP)

b. Internet Control Message Protocol (ICMP)

c. Centralizing Account Management (AAA)

d. Remote Command Line

Ans: Internet Control Message Protocol (ICMP)

28) Whose function is to screen network traffic for the purpose of preventing unauthorized access between computer networks?

a. Firewalls

b. Network Analysis

c. Documentation

d. None of the above

Ans: Firewall

29) Different types of software administrators are concerned about that could violate security policies.

a. Peer-to-peer file sharing

b. Web mail

c. Remote access

d. All of the above

Ans: All of the above

30) Which one of the following is not a Must-have Firewall feature?

a. Remote Access

b. Application Awareness

c. Granular Application Control

d. Bandwidth Management (QoS)

Ans: Remote Access

31) Which one is not the core function of a firewall?

a. Network Address Translation

b. Auditing and Logging

c. a & b both

d. None of the above

Ans: None of the above

32) What is the mask for IP address 192.168.0.0 as per Private Addresses specified in RFC1918?

a. 255.0.0.0

b. 255.240.0.0

c. 255.255.0.0

d. None of the above

Ans: 255.255.0.0

33) In which of the following way Modern Firewalls assist other areas of network quality and performance?

a. Enhance Network Performance

b. Intrusion detection and Intrusion Prevention

c. a & b both

d. None of the above

Ans: Intrusion detection and Intrusion Prevention

34) Which of the following is true

a. Firewalls are used to restrict access specific services.

b. Firewall cannot enforce security policies that are absent or undefined.

c. Firewalls can alert appropriate people of specified events.

d. All of the above

Ans: All of the above

35) Which layer holds the protocols for Telecommunicaton ?

a. Network layer

b. Physical layer

c. Data- link layer

d. Transport layer

Ans: Transport layer

36) Which of the following is a flaw of Data-link layer?

a. Battery operated

b. War driving

c. Evil Twin

d. Rogue Access Point

Ans: Battery operated

37) The threats to data link layer.

a. War chalking

b. WEP cracking

c. both a&b

d. None of the above

Ans: both a&b

38) Select the mitigation technique from the following.

a. Disabling unused services

b. Switch Security practices

c. Policies and procedures

d. All of the above

Ans: Policies and procedures

39) In which of the following way(s) wireless network security can be enhanced

a. Use a strong password

b. Enable your router firewall

c. Turn off Guest networking

d. All of the above

Ans: All of the above

40) Which of the following is/are fundamental component(s) of Wireless Intrusion Prevention System.

a. Sensors

b. Management Servers

c. Database server

d. All of the above.

Ans: All of the above

1) A network IDS is referred to as _____ .
   a. HIDS b. NIDS c. SIDS d. HIPS

   Ans: NIDS

2) Which of the following is/are Intrusion Detection (ID) system when it checks files and disks for known malware?
   a. Firewalls b. Antivirus c. Both a & b d. None of the above

   Ans: Both a&b

3) Which one of the following cannot be considered as an attack?
   a. Buffer Overflows
   b. Denial of Services
   c. Password cracking

d. Patching

Ans: Patching

4) _____ is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts.
   a. Stack-Based Intrusion Detection System (SIDS)
   b. Network Intrusion Decision System (NIDS)
   c. Host-Based Intrusion Detection System (SIDS)
   d. None of the above

   Ans: Network Intrusion Decision System

5) _____ identifies intrusion by analyzing system calls, application logs, file-system modifications and other host activities.
   a. Host-Based Intrusion Detection System (HIDS)
   b. Stack-Based Intrusion Detection System (SIDS)
   c. Network Intrusion Decision System (NIDS)
   d. All of the above

   Ans: Host-Based Intrusion Detection System (HIDS)

6) What kind of an activity the attacks are considered to be?
   a. All of the below
   b. Denial Of Service
   c. Unauthorized
   d. Buffer overflow

   Ans: All of the below

7) Which of the following mean “False Positive”?
   a. Incorrect ignorance of important events
   b. Incorrect escalation of unimportant events
   c. Correct ignorance of unimportant events
   d. None of the above

   Ans: Incorrect escalation of unimportant events

8) Which type of system is an evolution of HIDS ?
   a. Stack-Based Intrusion Detection System
   b. Network Intrusion Decision System
   c. Passive System
   d. Rective System

Ans: Stack-Based Intrusion Detection System

9) Which systems comes under Intrusion Prevention System (IPS)?
    a. Reactive Systems
    b. Active Systems
    c. Passive Systems
    d. All of the above

    Ans: Reactive System

10) Which of the following is true for Intrusion Detection System (IPS)?
    a. They are placed in-line
    b. They are able to actively block intrusions that are detected
    c. Takes actions such as sending an alarm, dropping the malicious packets, etc.
    d. All of the above

    Ans: All of the above

11) _____ is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management).
    a. SIEM
    b. SOAR
    c. UEBA
    d. None of the above

    Ans: SIEM

12) Which of the following is the most important feature to review when evaluating SIEM products?
    a. Testing
    b. Threat Intelligence feeds
    c. Aggregation
    d. All of the above

    Ans: Threat Intelligence feeds

13) Which protocol is used for VoIP?
a. Skype protocol
b. Media Gateway Control Protocol
c. Session Initiation Protocol
d. All of the above

Ans: All of the above

14) Which main function is performed by Media Server?
    a. Provisioning of Media connection
    b. Voicemail functionality
    c. Managing Digital Signal Processing (DSP)
    d. Free phone service

Ans: Voicemail functionality

15) Which main function is performed by Application server?
    a. Support of customized private dialing plans.
    b. Support of bandwidth policing mechanism
    c. Support of MGCP and MEGACO
    d. None of the above

    Ans: Support of customized private dialing plans

16) _____ switches calls between enterprises users on local lines while allowing all users to share certain number of external phone lines.
a. POT
b. PBX
c. TEM
d. All of the above

Ans: PBX

17) Which one of the following is considered to be in Computer Security classification?
a. Type A
b. Type D
c. Both a&b
d. None of the above

Ans: Both a&b

18) Which of the following defines Microsoft's Trust worthy computing technique?
    a. Memory curtaining
    b. Remote attestation
    c. Sealed storage
    d. All of the above

    Ans: All of the above

19) Which of the following is a hardware attacking vector?
    a. BIOS
    b. PBX
    c. POT
    d. None of the above

    Ans: BIOS

20) Which of the following does not define Jericho Security Model?
a. Integration
b. Simplifies use of public networks
c. It has a real open security framework
d. Aimed for open solution building blocks

Ans: It has a real open security framework

# SIC MULTIPLE CHOICE UNIT 4

1) What security device combines IOS firewall with VPN and IPS services?

   a. ASA

   b. ISR

   c. Cisco Catalyst switches

   d. IPS

   ANS: B.

2) Which of the following is a standards-based protocol for authenticating network clients?

   a. Cisco ISE

   b. PoE

   c. 802.1X

   d. CSM

   ANS: C.

3) The Cisco _____ is an integrated solution led by Cisco that incorporates the network infrastructure and third-party software to impose security policy on attached endpoints

a. ASA

b. CSM

c. ISR

d. ISE

ANS: D.

4) What software-based solution can network security administrators use to configure standalone ASA firewalls?

a. ISR

b. Cisco ISE

c. ASDM

d. IDM

ANS: C.

5) Cisco IOS Trust and Identity has a set of services that includes which of the following?

a. 802.1X

b. SSL

c. AAA

d. ASDM

ANS: A,B,and C.

6) IOS _____ offers data encryption at the IP packet level using a set of standards-based protocols.

a. IPS

b. IPsec

c. L2TP

d. L2F

ANS: B.

7) What provides hardware VPN encryption for terminating a large number of VPN tunnels for ISRs?

a. ASA SM

b. WebVPN Services Module

c. Network Analysis Module 3

d. High-Performance AIM

ANS: D.

8) What are two ways to enhance VPN performance on Cisco ISR G2s?

a. SSL Network Module

b. IDS Network Module

c. Built-In Hardware VPN Acceleration

d. High-Performance AIM

ANS: C and D

9) Which Cisco security solution can prevent noncompliant devices from accessing the network until they are compliant?

a. IPsec

b. ASA Service module

c. ACS

d. Cisco ISE

ANS: D.

10) Which of the following service modules do Cisco Catalyst 6500 switches support? (Select all that apply.)

a. ASA SM

b. Network Analysis Module 3

c. High-Performance AIM

d. FirePOWER IPS

ANS: A and B

11) What provides packet capture capabilities and visibility into all layers of network data flows?

a. Network Analysis Module 3

b. ASA Services Module

c. WebVPN Services Module

d. IPsec VPN SPA

ANS: A.

12) Which of the following are identity and access control protocols and mechanisms? (Select all that apply.)

a. 802.1X

b. ACLs

c. CSM

d. NetFlow

ANS: A and B.

13) Which two of the following are Cisco security management tools?

a. CSM

b. IDS module

c. ACS

d. Cisco ISE

ANS: A,C, and D.

14) True or false: NetFlow is used for threat detection and mitigation?

ANS: True

15) True or false: Cisco ASAs, ASA SM, and IOS firewall are part of infection containment.

ANS: True

16) What IOS feature offers inline deep packet inspection to successfully diminish a wide range of network attacks?

a. IOS SSH

b. IOS SSL VPN

c. IOS IPsec

d. IOS IPS

ANS: D.

17) What provides centralized control for administrative access to Cisco devices and security applications?

a. CSM

b. ACS

c. NetFlow

d. ASDM

ANS: B.

18) Match each protocol, mechanism, or feature with its security grouping:

i. CSM

ii. IGP/EGP MD5

iii. NetFlow

iv. Cisco ISE

a. Identity and access control

b. Threat detection and mitigation

c. Infrastructure protection

d. Security management

ANS: i = D, ii = C, iii = B, iv = A

19) What Is IDS?

a. Intrusion prevention system
b. Intrusions Detection system
c. Intrusion Detection system
d. Intrusion Decision system

ANS: C.

20) Types of IDS

a. Host based
b. Network based
c. Application based
d. All of the above

ANS: A and B.

21) what is IPS

a. Intrusion prevention system
b. Intrusions prevention system
c. Intrusion Project system
d. Intrusion Partition system

Ans :- A

22) Which Layer Use in hostbased IDS

a. Application layer
b. Network layer
c. Presentation layer
d. Transport layer

ANS: a.

23) Which Layer Use in Network based IDS

a. Application layer
b. Network layer
c. Presentation layer
d. Transport layer

ANS: B.

24) HIDS can detect what?

a. Traffic of implementation
b. Traffic of interest
c. Traffic of detection
d. None of these

ANS: B

25) ….. Includes denial of services, virus,worm ,infection ,buffer overflow , malfunction , file corruption , unauthorised program

a. IDS
b. IPS
c. Attack

d. Both a and b

ANS: C.

26) Four categories of misused? (select appropriate ans)

a. True positive
b. False positive
c. True Negative
d. False Negative
e. A and B
f. C and D

Ans: A,B,C, and D

27) IDS Tools Can track ?

a. Internal maliciousness
b. External attacks
c. Permanent maliciousness
d. Both a and b

Ans :- D

28) when an ids misses a legitimate thread know as ?

a. False positive
b. False negative
c. True negative
d. True positive

Ans :- B

29) ids are plugin with higher ?

a. True positive
b. False negative
c. False positive
d. True negative

Ans:-c

30 ) first generation ids focused on

a. Accurate attack detection
b. Backend option
c. Bountiful array
d. None of these

Ans :- a

31) **True Or false**

second generation ids detect attacks more than short them, prevent them , attempt to add value

Ans True

32 ) Hostbased IDS are static and dynamic

Ans :- true

33) two types of Hostbased IDS ?

a) File integrity
b) Behaviour monitoring
c) Static and dynamic
d) All of the above

Ans :- D

34) what was the file integrity?

a) Snap shot or checksum
b) Realtime monitoring
c) Behaviour monitoring
d) Sql Injection

Ans:- A

35) what was the behaviour monitoring

a) Snap shot or checksum
b) Realtime monitoring
c) Behaviour monitoring
d) None of these

Ans: B

36) behaviour monitoring on web server may monitor ?

a) Incoming request
b) Report maliciously

c) Html responses
d) Crossed side scripting attacks
e) Sql injection
f) A and D
g) C and E
h) All of the above

Ans: H

37) True or False

Network based ids they work By Capturing and analyzing network packet by on the wire

Ans:- True

38) network tabs dedicate appliances used to mirror a port or interface physically and swith port analysis are two most common methods of ?

a) Hostbased
b) Network based
c) Both A and B
d) None of these

Ans:- B

39) What are types of detection model ?

a) Anomaly model
b) Signature detection model
c) Both A and B
d) All of these

Ans:- C

40) anomaly detection IDS looks only at _____ ?\

a) Physical layer
b) Network packet
c) Network packet header
d) None of these

Ans :- C

41) anomaly detection IDS looks only at Network packet header is called protocol anomaly detection

Ans :- True

42) true or false

Signature detection or misuse IDS are the most popular types of IDS

Ans :- True

43) in signature detection model attacker is looking for the presence of ?

a) Buffer overflow
b) Particular file
c) Particular directory
d) Both A and B

Ans:- D

44) The shortest possible sequence detect is related thread in signature detection model what was needed ?

a) File
b) Directory
c) Bytes
d) None of these

Ans:- C

45) Disadvantages of IDS

a) Cannot recognize Unknown attack
b) Performance suffer as signature
c) Rules grow
d) All of the above

Ans:- D

46) what is fullform of SIEM

a) Security interface and event management
b) Security information and event management
c) Security information and event manager
d) Security interface and event manager

Ans :- B

47) feature of SIEM

a) Data aggregation
b) Analysis
c) Operation interface
d) Additional feature
e) A and C
f) B and D
g) All of the above

Ans:- G

48 ) what are the voice over Ip component

a) Call control elements
b) Gateway and gatekeepers
c) multi conference unit
d) Software clients and software end point
e) Contact center component
f) All of the above

Ans:- F

49) call control elements are runs on _____

a) Appliance
b) Hardware component
c) Server operating system
d) Software component

Ans :- C

50) voice and media gateway component is what allows

a) Termination to a PSTN
b) Transport in between TDM
c) Ip network
d) None of the above

Ans:- A_B_C

51) gatekeepers which kind of security function use

a) AAA
b) IP PBX
c) Both A and B
d) None of these

Ans:- A

52) what are hardware endpoint

a) Mobile device
b) eavesdropping
c) Denial of service attack
d) All of the above

Ans:- D

53) hardware endpoint by registering to the call control element

Ans: True

54) what are two reason of software endpoint

a) Cost
b) Softclient
c) Both a and B
d) None of the

Ans:- C

55) two component of  call center and contact center

a) Automatic call detection
b) Direct inward system
c) Interactive voice response
d) A and C

Ans:- D

56) what is PBX

a) Private branch exchange
b) Public branch exchange
c) Either a or B
d) All of the above

Ans :- A

57) feature of  PBX

a) Multiple extension

b) Voice mail
c) Remote control
d) Call forwarding
e) All of the above

Ans:-e

58) common attacks on PBX

a) Administrative ports and remote access
b) Voice mail denial of service
c) Securing PBX
d) All of the above

Ans:- D

59) what is TEM

a) Telecom expense management
b) Telegram expense manager
c) Telecom extended management
d) All of the above

Ans :- A

60) effort in involved the set of TEM

a) Increasing the cost
b) Optimize of the billing
c) Both A and B
d) None of these

Ans:- B

61) the operating system security model also known as trusted computing base

Ans: True

62) what are security model

a) Set of rules
b) Security functionality
c) Both A and B
d) None of these

Ans:- C

63) The operating system security model comes under ?

a) Network protocol layer
b) Security protocol layer
c) Physical security layer
d) All of the above

Ans:- A

64) what are vulnerable; to spoofing are trust relation between

a) Source address
b) Destination address
c) Ip address
d) Both A and B

Ans: D

65) ____ Is carried out Dos Attack

a) Source address
b) Destination address
c) Ip address
d) Both A and B

Ans:- C

66) what  is vulnerable to session Hijacking a

a) Attacker can take control of connection by the session key And Using it to insert is on traffic
b) Establish TCP IP communication session
c) Combination with dos Attack
d) Man in Middle attack
e) All of the above

Ans:- E

67) in sequence guessing number used in TCP connection is

a) 16 bits
b) 32 bits
c) 64 bits
d) 128 bits

Ans:- B

68) what is measure weakness of TCP IP

a) No authentication
b) No encryption
c) Both A and B
d) None of the above

Ans:- C

69) Different classing model

a) Bell-La-Padula
b) BiBa
c) Clark-wilson
d) All of the above

Ans:- D

70) Bell-La-Padula model consist of the following component

a) Set of subject
b) Set of object
c) Control metrics
d) None of the above

Ans :- A_B_C

71) the subject can only read the object

a) Read only
b) Append
c) Execute
d) Read-write

Ans :- A

72) The Subject can Only Write to The object but it can not be read

a) Execute
b) Read-write
c) Append
d) Read only

Ans:- C

73) Subject can execute the object but can neither read or write

a) Read -write
b) Read only
c) Execute
d) Append

ans :- C

74) subject has  both read and write permission to the object

a) Append
b) Read only
c) Execute
d) Read and write

Ans:- D

75) rules of biba model

a) Simple integrity ( no read down can not  read the data from lower integrity level )
b) Star integrity ( no write cannot write data to a higher integrity level
c) Invocation property ( can not invoke a subject at a higher integrity level )
d) All of the above

Ans:- D

76) what is acl

a) Access control list
b) Access define list
c) Access definition list
d) All of the above

Ans:- a

77) how many ACL component List

a) Discretionary access control list( DACL)
b) System access control list (SACL)

c) Rule based access control (RBAC)
d) Identity based access control ( IBAC)
e) All of the above

Ans:- E

78) what is DAC and What is MAC

a) Discretionary access control and mandatory access control list
b) Directory access control and mobile access control list
c) Both A and B
d) None of these

Ans:- A

79) Dac Is more Secure than MAc

Ans:- False

80 ) MAC is More Flexible

Ans:- False