SAMPLE QUESTION PAPER

1. ----------, cost reduction and portability are some significant benefits earned through the security program.
    a) Benchmarking
    b) Maturity rating
    c) FUD
    d) Business agility.
2. ---------- controls on network include audit trails and log files, system and network intrusion detection and prevention and security information and event management alerts.
    a) Detective
    b) Deterrence
    c) Defensive
    d) Security
3. The security ---------- represent business decision about what to do based on certain assumptions.
    a) Standards
    b) Procedures
    c) Policy
    d) Guideline
4. ---------- are day-today practices of individuals and technologies assigned to the protection of assets.
    a) Security Tactics
    b) Security technologies
    c) Security strategy
    d) Policy enforcement
5. Network --------- is the act of intercepting and monitoring your network traffic.
    a) Spoofing
    b) Phishing
    c) Attack
    d) Sniffing
6. System, network and application authentication controls can be carried out by --------- model.
    a) Lollipop
    b) Locked
    c) Onion
    d) Academic
7. ARP poisoning attack are form of ---------- attack that allow attacker to intercept and modify the network traffic invisibly.
    a) Denial of service
    b) ARP spoofing
    c) Network sniffing
    d) Man-in-middle.

8. ---------- authentication combines two or more credentials: what the user knows? what the user has? And what the user is.
    a) Single factor
    b) Two factor
    c) Triple factor
    d) Multifactor
9. In Kerberos authentication, Client send ---------- to KDC with request for the use of specific resource, and it include the fresh authenticator.
    a) KRB_TGS_REPLY
    b) TGT
    c) KRB_TGS_RESPONSE
    d) TGS.
10. A ---------- is collection of information that binds the identity (user, computer, service and device) to public key of public/private key pair.
    a) Sequential key
    b) One time password
    c) Time based key
    d) Certificates
11. In ----------, a subject's active role must be authorized for the subject.
    a) Role authentication
    b) Role assignment
    c) Permission authorization
    d) Role authorization
12. The advantage of port zoning is that, an intruder cannot connect host to switch, enable spoofing of good ---------- , and access LUN's of another host.
    a) Array
    b) WWN
    c) Port
    d) LUN
13. In ---------- risk, while performing deterrence, ensure the security policies include penalties for employees who access data they are not authorized for.
    a) Fraud
    b) Data leakage
    c) Storage persistence
    d) Inappropriate administrator access
14. Regular --------- of facilities should be done to ensure accountability for the all data sent offsite.
    a) Alterations
    b) LUN
    c) Audits
    d) Backup failure
15. In database administrator security, specific permissions are assigned to the ---------.
    a) Rules

b) Groups
c) Roles
d) Users

16. The database ---------- is special stored procedure that is run when specific actions occur within the database.
    a) View
    b) Trigger
    c) Revoke
    d) Trigger.
17. Application level security does not provide any type of protections for the users that can by pass ----------.
    a) Storage
    b) Application
    c) Server
    d) Network
18. Disadvantages while ---------- backup have the fastest backup time, they also boast the slowest data recovery time.
    a) Full
    b) Incremental
    c) Transaction log
    d) Differential
19. The best way to design and maintain the network that supports needs of that users is to involve network architecture and ---------- in application development process.
    a) Designer
    b) Tester
    c) Engineer
    d) Manager
20. The ---------- would typically include the perimeter router, Internet and all network attach to it.
    a) Parameterize network
    b) Intranet
    c) Demilitarize network
    d) Extranet
21. --------- : Uses firewalls,security aplliance,network segmentation and instrusion detection to manage and monitor access and information among networks.
    a) DS5.9
    b) DSS.10
    c) DS5.10
    d) DSS.9
22. ---------- is protocol for mapping an internet protocol address to physical machine address that is recognize in local network.
    a) TCP/IP protocol
    b) Address resolution protocol

c) Link state routing protocol
d) Distance vector protocol

23. ---------- have ability to connect dissimilar LANs on the same protocol.
    a) Switches
    b) Routers
    c) Hubs
    d) Gateways
24. An ---------- is collection of routers under a common administration such as company or an organization.
    a) Interior gateway
    b) Autonomous system
    c) Exterior gateway
    d) Dynamic routing
25. In distance vector routing protocol, ---------- is first generation Cisco proprietary protocol.
    a) RIPv1
    b) EIGRP
    c) RIPv2
    d) IGRP
26. ---------- can be configured to permit or deny TCP and UDP traffic based on source or destination address as well as other criteria like TCP and UDP port numbers contained in a packet.
    a) Patches
    b) AAA
    c) Access control list
    d) Routing table
27. ---------- agent helps in monitoring network performance, audit network usage, detect network faults or inappropriate access, and configure remote devices.
    a) AAA
    b) SNMP
    c) SSH
    d) ICMP
28. ---------- prevent unauthorized users from accessing private networks connected to the internet or intranet by examine each message passing trough the network.
    a) ACL
    b) Address resolution protocol
    c) Perimeter
    d) Firewall
29. ---------- provides disclosure of confidential materials through file attachment messages.
    a) Peer to peer file sharing
    b) Internet proxies
    c) Browser based file sharing

d) Web mails

30. ---------- antennas are typically used in point to multipoint wireless network topologies.
    a) Semi directional
    b) Bidirectional
    c) Omnidirectional
    d) Highly active
31. All 802.11 and 802.15 IEEE standards define wireless network employ ---------- technology.
    a) Spread spectrum band
    b) Bluetooth
    c) DSSS
    d) FHSS
32. ---------- is transmission technology in which data signals at the sending station is combined with high data rate bit sequence ,which divide user data based on spreading ratio.
    a) Spread spectrum band
    b) Bluetooth
    c) DSSS
    d) FHSS
33. ---------- wireless network can function in both circuit-switching and packet-switching modes which can be used simultaneously.
    a) Spread spectrum band
    b) Bluetooth
    c) DSSS
    d) FHSS
34. In Bluetooth, --------- is cable replacement protocol that interfaces with core Bluetooth protocol.
    a) SDP
    b) L2CAP
    c) LMP
    d) RFCOMM
35. On wireless network, inspection involves ---------- in which the intruder shamelessly listening for wireless packet using tools and begin developing footprint of wireless network.
    a) Spoofing
    b) Filtering
    c) Sniffing
    d) Phishing
36. EAP-LEAP uses modified MS-CHAPv2 with insecure ---------- hashing and weak DES selection.
    a) MD5
    b) AES

c) MD4
d) EAP

37. ---------- layer is topmost layer of OSI model.
    a) Session
    b) Presentation
    c) Application
    d) Physical.
38. ---------- is an event when no attack has taken place and no detection is made.

    a) True positive
    b) False positive
    c) True negative
    d) False negative
39. ---------- can prevent known attacks, or shut down access to internal machine from external host when it detects a probe or an attack.
    a) Firewall
    b) IPS
    c) IDS
    d) Normalizer
40. ---------- is ineffective during DoS attacks.

    a) HIPS
    b) NIDS
    c) HIDS
    d) NIPS
41. ---------- can be made very secure against attack and even made invisible to many attackers.

    a) HIPS
    b) NIDS
    c) HIDS
    d) NIPS
42. The --------- works behind the firewall and provides analysis layer that scans traffic and reports back on threats.

    a) Sniffing tool
    b) IPS
    c) IDS
    d) Normalizer
43. The basic part of SIEM includes collection, analysis/aggregation and ----------.
    a) Reporting
    b) Alert
    c) Retention

d) Documenting

44. ---------- has features like automated call distribution, interactive voice response system, outbound dialers, call recording system .

    a) Gateway-gatekeeper
    b) Contact center components
    c) Call control elements
    d) Software endpoints

45. During traditional carrier network, switches were introduce by class hierarchy in which ---------- tandem switches interconnecting whole regions.

    a) Class 2
    b) Class3
    c) Class 4
    d) Class 5

46. The major function of ---------- is analog-to-digital conversion of voice.
    a) call processing server/IP PBX
    b) user end devices
    c) media/VOIP gateways
    d) IP network

47. Media Gateway control protocol privides a signalling and control protocol between VoIP gateway and ---------- gateway.
    a) PBX
    b) ISDN
    c) PSTN
    d) ITU

48. ---------- SPECIFIES CALL CONTROL.

    a) H.225
    b) H.323
    c) H.245
    d) H.450

49. In -------, authentication and authorization are handled by either on request by request basis with challenge/response mechanism, or by using lower layer scheme.
    a) MGCP
    b) PBX
    c) SIP
    d) TEM

50. Attackers hack -------- to place outgoing calls that are charged to the organization's account.

    a) MGCP
    b) PBX

c) SIP
d) TEM

51. TEM is offered as ---------- where vendors are able to target net saving for clients.
    a) Infrastructure as services
    b) Platform as services
    c) Software as services
    d) Voice as services
52. ---------- rule state that subject at one level of confidentiality is not allowed to wite information to a lower level of confidentiality.
    a) Simple security
    b) Star* security
    c) Strong star*
    d) Security star*
53. Trustworthy computing is based on four pillars: security, ----------, privacy and business integrity.
    a) Reference
    b) Confidentiality
    c) Reliability
    d) Availability
54. ---------- helps in reducing side-channel attacks which cracks encryption algorithm with the help of hardware.

    a) Cloud computing
    b) Hypervisor
    c) VMware
    d) VMM
55. In ----------, direct access to host's network interface cards independent of host OS is given to the guest OS.
    a) Network bridging
    b) Network address translation
    c) Host only networking
    d) Host only networking
56. ---------- helps in delivering software application on subscription basis over the internet.

    a) IAAS
    b) PAAS
    c) SAAS
    d) Cloud computing
57. ---------- cause by physical access is different between large cloud service providers and their customers.
    a) Change management
    b) Denial of service threat

c) Physical disruption
d) Exploiting weak recovery

58. ---------- is a technique applied to threat scenarios which help a team in identifying security vulnerabilities and risk.
    a) Secure design
    b) Threat monitoring
    c) Secure coding
    d) Security testing
59. ---------- request forgery is an attack that results in an unsought transfer of funds,change passwords or data theft.

    a) Cross-site scripting
    b) SQL injection
    c) Cross site request forgery
    d) Malicious file execution
60. Applications needs to be updated with the latest release and security patches to maintain ----------.

    a) Security
    b) Authenticity
    c) Authorization
    d) Integrity
61. Using ---------- encoding, the browser encode username and password and send it back to server. If login is correct, the server returns message number 200 and if it fails, it replies with the same 401 error as before.
    a) MD5
    b) SSL
    c) BASE64
    d) DES
62. ----------method is used to verify that the person accessing the system is human being with the help of distorted image of letters and numbers.

    a) MD5
    b) CAPTCHA
    c) BASE64
    d) SSL
63. Servers, NAS-SAN, desktop, laptops, tablets, pads, projectors are the ----------.
    a) Computer equipment
    b) Communication equipment
    c) Technical equipment
    d) Storage media

64. File cabinets containing sensitive information or valuable equipment's should be kept ---- ---------- when not in used.
    a) In server
    b) Authenticated
    c) Locked
    d) Authorized
65. A ---------- device uses distinctive personally identifiable characteristics or unique physical traits to positively identify the individual.
    a) CAPTCHA
    b) Authenticator
    c) Biometric
    d) Credential
66. It should be warranted that the cabling used for ---------- device is not readily accessible, so that no one can easily tap into transmission or tamper the device to stop or block the process.

    a) CAPTCHA
    b) Biometric
    c) CCTV
    d) Alarms
67. Points of entry and exit should be fitted with intrusion ----------.
    a) CAPTCHA
    b) Biometric
    c) CCTV
    d) Alarms
68. Some CISO use industry ---------- as measures for their own spending while those can be used as informative reference point.
    a) FUD
    b) Maturity rating
    c) Benchmark
    d) VPN
69. ---------- is ongoing strategy for providing head count needed to operate security function.
    a) Resouce plan
    b) Roadmap
    c) Risk analysis
    d) Remediation plan
70. ---------- refers to providing access to data only to those who are authorized to use it.
    a) Integrity
    b) Confidentiality
    c) Availability
    d) Defense model.

71. Managing your applications and their security should be top priority of any ----------.
    a) Manager
    b) Administrator
    c) Designer
    d) Host
72. ---------- allow the use of passwords by organizations that require increase security for remote wireless 802.1x authentication but that do not have PKI support password.
    a) EAP/TLS
    b) EAP/CHAP
    c) EAP/SSL
    d) EAP/MD5-CHAP
73. A ---------- is which verifies the identity of entities requesting their digital certificates to be stored at CA.
    a) Root CA
    b) Registration authority
    c) Intermediate CA
    d) Issuing CA
74. ---------- mechanism allows multiple host to communicate with the array and only access LUN that are assigned through application that provide protection.
    a) LUN unmasking
    b) Port zoning
    c) Risk remediation
    d) LUN masking
75. Once network security system is created and implemented, the system needs to be ---------- to determine if current system i.e appropriate for the network it is protecting.
    a) Tested
    b) Modified
    c) Design
    d) Analyzed
76. When customer records the changes , corresponding changes can be easily made by calling ----------.
    a) Triggers
    b) Store procedures
    c) ER diagram
    d) Views.
77. In ---------- security, by limiting numbers of actual accounts that have database access, limit your exposures to external hacking attempt.
    a) Storage
    b) Application
    c) Server
    d) Network
78. ---------- is normally used to separate the inside network and outside world.
    a) Perimeter

b) Firewall
c) Switches
d) Router

79. ---------- : Establish wireless robust security network.
    a) SP 800-97
    b) SP 800-153
    c) SP 800-48
    d) SP 800-120
80. MAC address are 6 byte in length, first 3 bytes are ------ number of manufacturer which are assign by internet standard body and second 3 bytes are the serial number assign by manufacturer.
    a) IP
    b) Serial
    c) ID
    d) Sequential
81. Applying vendor security patches regularly is first step to help ---------- your computing system.
    a) Secure
    b) Discovering
    c) Harden
    d) Networking
82. ---------- provides mechanism for reporting TCP/IP communication problems and utilities for testing IP layer connectivity.
    a) AAA
    b) SNMP
    c) SSH
    d) ICMP
83. In --------, many private IP addresses can be translated to single public IP address.
    a) NAT
    b) SAT
    c) PAT
    d) MAT
84. Spread spectrum refer to ---------- low power transmission, as opposed to narrowband transmission.
    a) Low frequency
    b) Wide bandwidth
    c) Low bandwidth
    d) Wide frequency
85. Listening for the beacon frames sent by access point or adhoc wireless host on all channels is called as ---------- scanning.
    a) Active
    b) Static
    c) Passive

d) Dynamic

86. ---------- allows users to access the internet and other resources provided by the access point, excluding LAN capability.
    a) Wireless phishing
    b) Client isolation
    c) Misconfigure access point
    d) Rogue access point
87. A ---------- is wireless access point installed on wired network without authorization from network administration.
    a) Wireless phishing
    b) Client isolation
    c) Misconfigure access point
    d) Rogue access point
88. ---------- analyze network traffic and system-specific setting such as software calls, local security policy, local log audit and more.
    a) HIPS
    b) NIDS
    c) HIDS
    d) NIPS
89. During traditional carrier network, switches were introduce by class hierarchy in which ---------- switches connecting subscribers and end users.
    a) Class 2
    b) Class3
    c) Class 4
    d) Class 5
90. In ----------, the owner of the object specifies which subjects can access the object.
    a) Mandatory access control
    b) Subjective access control
    c) Discretionary access control
    d) Media access control
91. ---------- includes contacting people for verifying and diagnosing the issue and fixing them.

    a) Security documenting
    b) Security release management
    c) Dependency patch monitoring
    d) Product security incident response
92. Routers, switches, firewalls, modems, PBX, fax machine, video conference system, TV are the ----------.
    a) Computer equipment
    b) Communication equipment
    c) Technical equipment
    d) Storage media

93. ---------- means that software and data can be used on multiple platform or can be transfer or transmitted within the organization to customer or to the business partners.
    a) Business agility
    b) Cost reduction
    c) FUD
    d) Portability
94. If you attempt to download malware, ---------- scanning will catch it immediately and not allow it to damage your system.
    a) Manual
    b) Virus
    c) Real time
    d) Performance
95. A central server can validate given ---------- ,since its clock is synchronized with the token and it knows the user's pin.
    a) Password
    b) Token
    c) Pin
    d) Username
96. Transport layer security is internet standard version (RFC2246) of the proprietary --------.
    a) Kerberos
    b) One time password
    c) SSL
    d) Time based key
97. In the detection mechanism of ----------, use integrity checking software to monitor and report alterations to key data will be carry out.
    a) Data corruption
    b) Hijacking
    c) Accidental modification
    d) Fraud
98. Distribution layer would contain intermediate switches and routers such as those use to route between subnet and ----------.
    a) Firewall
    b) Layer 2 VLAN
    c) Hubs
    d) VLAN
99. ---------- need to be selected on the basis of business context, so they are targeted towards specifically identified risks with clear objective.
    a) Security Tactics
    b) Security technologies
    c) Security strategy
    d) Policy enforcement
100. In securing storage components, we must have to account three primary categories which are, storage network, --------- and servers.

a) Disks
b) Storage device
c) Array
d) SAN