الجمهورية اليمنية
جامعة صنعاء

قائمة الاسئلة

امتحان نهاية الفصل الدراسي الثاني - للعام الجامعي 1446 هـ - الموافق -2025/2024م-كلية الحاسوب وتكنولوجيا المعلومات :: اساسيات الا

د. عبدالواسع العزاني

1) A very important network protocols commonly adopted in the modern network communication are …………..
   1) + Ethernet, TCP/SPX, Internet Protocol (IP), HTTP/FTP, DNS and SMTP
   2) - World Wide Web (WWW), HTTP, Switches, Hubs
   3) - HTTP/FTP, DNS, SMTP, World Wide Web (WWW), HTTP
   4) - Ethernet, TCP/SPX, Internet Protocol (IP), Switches, Hubs
2) The networks can be classified into the ……………. irrespective of their coverage area.
   1) - Local area network (LAN), Wide area network (WAN), Wireless, Wired
   2) - Metropolitan area network (MAN), Wide area network (WAN), Wired, Wireless
   3) - Local area network (LAN), Metropolitan area network (MAN), Wired, Wireless
   4) + Local area network (LAN), Metropolitan area network (MAN), Wide area network (WAN)
3) ……….. is the name of the combination of both web users and the resources that use the HTTP for communication.
   1) + World Wide Web (WWW)
   2) - Internet
   3) - Server
   4) - Router
4) ………… is an application-level protocol that communicates with the server through user agents such as web browsers, mobile apps, voice browser, web crawlers, and other similar kinds of client software agents.
   1) - World Wide Web (WWW)
   2) + HTTP
   3) - Internet
   4) - Server
5) The ………… works on the network, transport, and session layers of the seven-layer OSI model.
   1) - HTTP
   2) - Internet
   3) - Server
   4) + TCP/IP suite
6) The ……….. is managed and governed by the International Assigned Number Authority (IANA).
   1) - HTTP
   2) - DNS server
   3) - TCP/IP
   4) + IP address
7) The ………… are normally connected to the edge routers through Gigabit Ethernet copper or fiber cables.
   1) - hosts
   2) - switches
   3) + routers
   4) - hubs
8) The ………….. is normally connected after edge router inside the local network.
   1) + firewall
   2) - core router
   3) - edge router
   4) - server
9) The ……………… is the general name of the entire infrastructure of the Internet.
   1) - core router
   2) - firewall

3) - edge router
4) + Internet cloud

10) The …………. is the protection of software, hardware, and data resources connected and stored on the Internet.
1) + cybersecurity
2) - information security
3) - data confidentiality
4) - data integrity

11) The main sources of breach of the availability are ………………..
1) - choking of data bandwidth, introduction of malware on the server, manipulation of original data, introduction of viruses, malicious insiders
2) - theft of employee laptops, manipulation of original data, introduction of viruses, malicious insiders
3) + choking of data bandwidth, failure of hardware, malfunction of software, redundant arrangement failures
4) - theft of employee laptops, leaving computers with confidential information unattended, providing unauthorized access to the unconcerned person, unauthorized access by hacker through malware

12) The main sources of breach of the confidentiality are ………………..
1) - choking of data bandwidth, introduction of malware on the server, manipulation of original data, introduction of viruses, malicious insiders
2) + theft of employee laptops, leaving computers with confidential information unattended, providing unauthorized access to the unconcerned person, unauthorized access by hacker through malware
3) - theft of employee laptops, manipulation of original data, introduction of viruses, malicious insiders
4) - choking of data bandwidth, failure of hardware, malfunction of software, redundant arrangement failures

13) The main sources of breach of the integrity are ………………..
1) - theft of employee laptops, leaving computers with confidential information unattended, providing unauthorized access to the unconcerned person, unauthorized access by hacker through malware
2) - theft of employee laptops, manipulation of original data, introduction of viruses, malicious insiders
3) - choking of data bandwidth, failure of hardware, malfunction of software, redundant arrangement failures
4) + introduction of malware on the server, manipulation of original data, introduction of viruses, malicious insiders

14) ……………… must be informed and flexible to identify and manage potential new threats effectively.
1) - Board of Directors
2) - Senior Information Security Management
3) + Cybersecurity professionals
4) - Cybersecurity Practitioners

15) Three common controls used to protect the availability of information are: ……………
1) + Redundancy, backups and access controls.
2) - Encryption, file permissions and access controls.
3) - Access controls, logging and digital signatures.
4) - Hashes, logging and backups.

16) Governance has several goals, including: ……………..

1) + Providing strategic direction, Ensuring that objectives are achieved, Verifying that organizational resources are being used appropriately, Ascertaining whether risk is being managed properly.
2) - Directing and monitoring security activities, Access controls, Encryption, file permissions and access controls.
3) - Providing strategic direction, Ensuring that objectives are achieved, Ascertaining whether risk is being managed properly, Encryption, file permissions and access controls.
4) - Providing strategic direction, Ensuring that objectives are achieved, Verifying that organizational resources are being used appropriately, Hashes, logging and backups.

17) According to the NIST framework, which of the following are considered key functions necessary for the protection of digital assets?
1) - Identify, Recover, Investigate, Encrypt, Govern
2) + Identify, Protect, Recover, Detect, Respond
3) - Investigate, Identify, Protect, Recover, Govern
4) - Recover, Detect, Investigate, Govern, Access control

18) Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation?
1) - Board of directors
2) - Executive committee
3) - Cybersecurity practitioners
4) + Cybersecurity management

19) The risk Assessment include: ……………..
1) + Secure Code Scan, Data-Centric Risk Assessment, Vulnerability Scan, Penetration Test
2) - Third Party Risk, Company's Written Supervisory Procedures, Awareness, Training
3) - Data-Centric Risk Assessment, Vulnerability Scan, Executive Management,
4) - Secure Code Scan, Penetration Test, Laws and Regulations, Audit.

20) Central to this awareness is …………… that affect information security.
1) + an understanding of key business and technology factors
2) - economy of mechanism and fail-safe defaults
3) - perimeter security controls and applications security controls
4) - cybersecurity standards and economy of mechanism

21) The security principles include: …………………
1) - A.Economy of mechanism, Fail-safe defaults, Complete mediation, Open design, Separation of privilege
2) - B.Least privilege, Least common mechanism, Psychological acceptability, Work factor, Compromise recording.
3) - C.understanding of key business, technology factors, economy of mechanism, fail-safe defaults, perimeter security controls
4) + a and b

22) ………………. states that all access to all objects must be checked to ensure that they are allowed.
1) + Complete mediation
2) - Least privilege
3) - Least common mechanism
4) - Separation of privilege

23) …………….... is the security architecture and design of a system should be made publicly available.
1) - Psychological acceptability
2) - Work factor
3) + Open design
4) - Compromise recording

24) …………… principle states that the price of circumventing a security mechanism should be compared with the resources of a possible attacker when designing a security scheme

1) - Separation of privilege
2) + Work factor
3) - Open design
4) - Compromise recording

25) ………….. are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the information security.

1) - Awareness and training
2) - Access controls
3) - Security principles
4) + Security policies

26) …………… is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information.

1) + An information security policy
2) - Access controls
3) - Security principles
4) - Security policies

27) ……………. clarify functional and assurance steps that should be taken to achieve the objectives of the organization in terms of cybersecurity.

1) - An information security policy
2) - Access controls
3) + Cybersecurity standards
4) - Security principles

28) …………………. standard deal with the IT control within the IT organizations.

1) - Information Security Forum (ISF)
2) + ISO/IEC 2700x
3) - Payment Card Industry Data Security
4) - a and b

29) …………….. is(are) he combination of the probability of an event and its consequence

1) + Risk
2) - Threat
3) - Vulnerability
4) - Asset

30) The different approaches to implementing cybersecurity include: ……………

1) - Threat agents, governance, compliance and mobile device policy.
2) - Network configuration, navigation controls, user interface and VPN traffic.
3) + compliance-based security, risk-based security, ad hoc security
4) - Isolation, segmentation, internal controls and external controls

31) Cybersecurity risk management is a continuous and iterative process that involves several key elements: ………………..

1) - Risk Treatment, Network configuration, navigation controls, user interface and VPN traffic
2) + Asset Identification, Threat Identification, Vulnerability Assessment, Risk Assessment, Compliance, Monitoring and Review
3) - Risk Assessment, Compliance, Isolation, segmentation, internal controls and external controls
4) - Risk Treatment, Network configuration, Threat agents, governance, compliance and mobile device policy.

32) Many computers from different parts become the part of ………. attack without any approval and

knowledge of the owner of the computer.

1) - DoS
2) - Man-in-the-Middle
3) - Spamming
4) + DDoS

33) …………….. is the illegal or fraudulent use of the digital resources like software and digital content.

1) + Digital Property Misappropriation
2) - Man-in-the-Middle
3) - Spamming
4) - Phishing

34) ……………… is a type of malware that restricts your access to systems and files, typically by encryption and then demands a ransom to restore access.

1) + Ransomware
2) - Cyber frauds and forgery
3) - Cyberstalking
4) - Digital or cyber vandalism

35) The number and types of layers needed for defense in depth are a function of: …………..

1) + Asset value, criticality, reliability of each control and degree of exposure.
2) - Threat agents, governance, compliance and mobile device policy.
3) - Network configuration, navigation controls, user interface and VPN traffic.
4) - Isolation, segmentation, internal controls and external controls

36) Which of the following statements about advanced persistent threats (APTs) are true?

1) - APTs typically originate from sources such as organized crime groups, activists or governments.
2) - APTs use obfuscation techniques that help them remain undiscovered for months or even years.
3) - APTs are often long-term, multi-phase projects with a focus on reconnaissance.
4) + All in above (a, b, c)

37) Which three elements of the current threat landscape have provided increased levels of access and connectivity, and therefore increased opportunities for cybercrime?

1) - Text messaging, Bluetooth technology and SIM cards
2) - Web applications, botnets and primary malware
3) - Financial gains, intellectual property and politics
4) + Cloud computing, social media and mobile computing

38) ……… is a ransomware crypto worm, which targeted computers (when it first appeared) running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

1) + WannaCry
2) - Ransomware
3) - Cyber frauds and forgery
4) - Cyberstalking

39) ……………… is basically an unwanted software or programming code that runs on a computer and may cause harm or jeopardize the normal functions of a computer.

1) - WannaCry
2) + A malware
3) - Ransomware
4) - Cyber frauds and forgery