Networked Application Assignment

1. a) A software program that requires a network (LAN, WAN, or the Internet) to function. Examples include web browsing, email, messaging apps, and cloud services.

   b) How application layer work is divided among devices, such as client/server, peer-to-peer, distributed, or standalone systems.

   c) It is widely used for web browsing, email, and most online services.

   d) Massively increasing client processing power (Moore's Law), which makes clients powerful enough to act as servers.

   e) The consolidation of servers into fewer, more powerful, centralized systems.

2. a) Because compromising an application allows them to bypass network protections and directly control resources.

   b) They can fully control the computer, install malware, read/modify files, or control system processes.

   c) More apps equals more vulnerabilities, and mobile devices often lack strong security protections.

3. a) Because reflected input may contain malicious scripts (XSS), which can execute on the website and harm users.

4. a)
   Physical servers: Hardware machines with their own OS and resources.
   Virtual machines (VMs): Software created computers running on top of physical servers, each with its own OS and IP address.

   b) Rapid creation, deletion, cloning, scaling, and isolation. Also flexible resource allocation.

5. a) Their applications, settings, and data follow them automatically through the cloud.

   b) Encryption, backup, redundancy, and access control to protect stored files.

6. a) They cannot control the provider's security and risk catastrophic data loss if the provider fails. Due diligence is required.

7. a) It greatly increases network traffic and creates rapid, unpredictable changes. Reliability and bandwidth demands rise.

   b) Many AI interactions (e.g., voice assistants) need near instant processing; latency disrupts performance.

8. a)
   Standards for transferring files (e.g., HTTP).
   Standards for file formats (e.g., HTML, image formats).

   b)
   Transfer standards move data between devices.
   Format standards define how the content is structured and displayed.

9. a) STMP

   b) HTTP

10. a) POP or IMAP

    b) HTTP

11. a) The idea of brief, immediate, mobile messaging that later led to modern messaging apps.

    b) Through attachments, such as Word documents or other formatted files.

12. a) It only protects the first link and not the entire path through all mail hosts.

    b) Link encryption: Protects each link separately.
    End-to-end encryption: Encrypts between the two clients directly.

    c) Each mail host decrypts and re-encrypts messages, exposing them at every stop.

    d) Use end-to-end encryption so only the sender and receiver can decrypt.

e) Requires both parties to use the same system and digital certificates, making setup difficult.

13. a) Voice over Internet Protocol and Voice over IP networks (the general technology).

14. a) Digitize (encode) voice signals
Convert received digital signals back to audio

b) The amount of data transmitted but often at the cost of voice quality.

15. a) Software clients (apps)
Hardware VoIP phones

b) Translate between VoIP networks and traditional telephone networks.

16. a) Signaling protocol.
b) A client contacts a SIP proxy server, which helps set up the call. Then the devices communicate directly for voice.

17. a) Digitized voice samples

b) RTP over UDP.

c) Packet sequencing and Timing/synchronization issues

18. a) Low cost and scalability, new peers add capacity instead of consuming it.

b) Clients may not always be online
Clients change IP addresses
Security concerns
High resource usage

19. a) Yes, by encrypting through multiple nodes.

b) Yes, by hiding the sender's identity through layered routing.

c) Removes one layer of encryption and forwards the message to the next router.