Network Defense Essentials (NDE)

1. Which of the following objectives of cryptography defines the trustworthiness of data or resources to prevent improper and unauthorized changes?

A. Nonrepudiatio

B. Authentication

**C. Integrity**

D. Confidentiality

1. Which among the following is not a step involved in the creation of a data backup strategy/plan?

A. Identifying an encryption plan.

B. Conducting a recovery drill test.

C. Choosing the right backup solution.

**D. Selecting the appropriate RAID levels.**

3. Which of the following authorization techniques refers to gaining access to the requested resources and obtaining permission to access the resources attached with the primary requested resource?

**A. Centralized authorization**

B. Decentralized authorization

C. Implicit authorization

D. Explicit authorization

4. Which of the following tiers of an IoT-enabled IT environment focuses on data computation to deliver insights and thereby generate business value?

A. Gateway tier

**B. Cloud tier**

C. Device tier

D. Control tier

5. Which of the following suspicious traffic signatures exposes malicious attempts such as ping sweep, port scan, and DNS querying?

A. Informational

B. Unauthorized access

C. Denial-of-service (DoS)

**D. Reconnaissance**

6. Which of the following sentences is NOT an advantage of network traffic monitoring?

A. Detecting signs of malicious activity.

**B. Determining download/upload speeds.**

C. Increasing bandwidth bottlenecks.

D. Investigating security breaches.

7. Which of the following security controls discourages entities from policy violations and sends warning signs if any policy violations are reported?

A. Prevention controls

B. Encryption and protocols

**C. Detection controls**

D. Deterrence controls

8. Steve deployed a security solution that encrypts and allows accessing, transmitting, or storing important information on only authorized apps using strong password protection policies, without compromising on speed. Identify the solution employed here.

A. Metasploit

**B. Vaultize**

C. Tor's Hammer

D. zANTI

9. Which of the following layers in the IoT architecture allows businesses to make a decision based on the information derived from policies and procedures of IoT computing?

A. Cloud platform layer

B. Process layer

C. Communication layer

D. Device layer

10. Identify the Internet access policy that enables only safe/necessary services individually, and nonessential services/procedures that cannot be made safe are not allowed.

A. Promiscuous policy

**B. Prudent policy**

C. Paranoid policy

D. Permissive policy

11. Finch segregated the LAN creating an independent subnetwork that has been placed between organization’s internal network and outside public network to enable high-level protection for LAN. Identify the independent network created to protect the LAN.

A. Honeypot

B. Proxy server

**C. DMZ**

D. VLAN

12. Kristen deploys firewall in his organization that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate or not. Identify the firewall technology implemented here.

**A. Circuit-level gateways**

B. Stateful multilayer inspection firewall

C. Application-level gateways

D. Application proxy

13. Which of the following terms refers to the actions performed by a user on a file or a process to change its state through the given permission?

**A. Operation**

B. Subject

C. Object

D. Reference monitor

14. Which of the following cloud deployments is a dynamic heterogeneous environment that combines workloads across various cloud vendors and is managed via one proprietary interface to achieve long-term business goals?

A. Public cloud

**B. Multi cloud**

C. Private cloud

D. Community cloud

15. James, accessed a booking portal to book a ticket. As he does not have an account in that platform, he got a pop-up message informing him to access through any social media account. Identify the authentication method demonstrated in the scenario.

A. Biometric authentication

B. Smart card authentication

C. Single sign-on (SSO) authentication

**D. Two-factor authentication**

16. Which of the following encryption algorithms is used in Wi-Fi Protected Access 2 (WPA2) encryption for securing the wireless network?

A. RC4, TKIP

B. RC4

**C. AES-CCMP**

D. AES-GCMP 256

17. Which of the following physical security systems allows only one person inside and requests an identity; if the identity is invalid, the person is held inside until a security professional arrives?

A. Walkthrough detectors

B. X-ray inspection systems

C. Metal detectors

**D. Mantrap systems**

18. Which of the following protocol employs a client–server model and provides authentication, authorization, and accounting (AAA) for remote-access servers to communicate with a central server?

A. HTTPS

**B. RADIUS**

C. IPsec

D. SMTP

19. Identify the title of the Digital Millennium Copyright Act that implements the World Intellectual Property Organization (WIPO) treaties.

A. Title V

B. Title II

**C. Title I**

D. Title III

20. Which of the following is an open-source technology that provides PaaS through OS-level virtualization and delivers containerized software packages?

A. Microservices

B. Serverless computing

**C. Docker**

D. Virtual machines

21. To check whether the organization’s data is plagiarism free, Stephen implemented a security policy that defines a set of rules for storing and maintaining the data for operational and regulatory purposes. Identify the security policy used here.

A. Data backup policy

B. Acceptable use policy

**C. Data retention policy**

D. Internet usage policy

22. Which of the following components of a wireless network is used to connect systems to a wireless network and access the Internet directly with the help of an ISP?

A. Wireless repeater

B. Wireless bridge

C. Wireless NIC

**D. Wireless modem**

23. John identified a suspicious activity while monitoring the IDS screen and subsequently performed automated counteraction, and blocked hacker’s further activity on the organizations network. Identify the intrusion detection step used here.

A. IDS responds.

B. Alert message sent.

**C. The administrator assesses the damage.**

D. Events are logged and reviewed.

24. Which of the following systems is used in industries and warehouses to identify a fire incident before the fire spreads and alerts the occupants with an alarm?

A. Fire extinguisher system

B. Fire protecting system

C. Fire suppression system

**D. Fire detection system**

25. Which of the following technologies is referred to as a wireless sensor protocol that enables communication between sensors and their controllers?

A. USB

B. Satcom

C. GPS

**D. ANT**