19. A hospital's network hosts sensitive patient records and a public-facing appointment booking website. To protect the internal database, the IT team configures a firewall to block all incoming traffic except for HTTP/HTTPS requests to the booking server. The firewall also prevents staff from accessing unauthorized external websites.

(i) Rearrange the following steps to implement and configure firewall techniques in a network security system.

Step 1: Configure Packet Filtering
Step 2: Create a DMZ Zone
Step 3: Test and Monitor traffic
Step 4: Define Security Policies
Step 5: Implement Stateful Inspection

(ii) Whether the above scenario for firewall techniques can be automated using scripts, management consoles, or security platforms to monitor, control, and respond to network traffic. Justify the reason.

20. An intruder attempts to gain access to the textile industry Zigbee network using a malicious device, the firewall detects and filters out unauthorized traffic based on predefined security rules.
Assess how IDS and encrypted communication help ensure a secure and fraud-free online purchase of machineries for textile mills instead of relying on firewall detections.

21. Complete the following statements for the firewall design process.
A. Identify network assets: Establish what needs to be protected and its value to the organization.
B._________: Determine what traffic should be allowed or denied according to organizational requirements.
C._________: Convert policies into specific allow/deny rule sets within the firewall.
D._________: Validate the firewall setup in a controlled environment and move it into production.
E. _________: Continuously track firewall activity to detect suspicious behavior or potential breaches.
F. Regularly update and audit firewall configuration: Ensure firewall rules, firmware, and policies are kept current and secure
against evolving threats.

22. Identify the specific misconfiguration involved for the below scenario based on the hint given and justify the reason for a security risk.
Hint: Outdated firmware, Tufin, Qualys Guard, Default credentials, Weak encryption, SolarWinds Network Configuration, Unrestricted access.

Scenarios:
a) The firewall firmware has not been updated in over three years.
b) The company uses "admin/admin" as the default login credentials for all firewalls and routers.
c) The Wi-Fi network uses outdated WEP encryption in a corporate environment.
d) All firewall ports are left open without applying any IP filtering for convenience.
e) The company uses anonymous as the default login credentials for all firewalls and routers.

23. Identify the design principle required for a marketing company to secure its network so that only trusted traffic is allowed and the firewall stays intact. Provide real world example for the same.

24. During a major online sale event, a customer at flipkart.com uses their credit card to purchase electronics. Explain how the SET (Secure Electronic Transaction) protocol ensures a secure and trusted transaction between the customer, the merchant, and the bank.
(i) Illustrates the workflow of Secure Electronic Transaction (SET) protocol during an online payment process in flipkart website to ensure security.
(ii)Identify the correct answer and justify it. (2 Marks)
Assertion (A): Secure Electronic Transaction (SET) protocol ensures that payment information is shared directly with the merchant.
Reason (R): SET does not use dual signature and encryption to separate order information and payment details, therefore confidentiality and data integrity is not maintained.
A. Both Assertion and Reason are true, and the Reason is the correct explanation of the Assertion.
B. Both Assertion and Reason are true, but the Reason is not the correct explanation of the Assertion.
C. Assertion is true, but Reason is false.
D. Assertion is false, but Reason is true.

25. Identify the correct order of phishing attack.
(i)The victim enters sensitive information on a fake webpage.
(ii)The attackers design a convincing email to lure the victim.
(iii)The stolen information is used for unauthorized access or fraud.
(iv)The victim clicks a malicious link and is redirected to a fake webpage.

26. Provide the five data hiding techniques from access control to long term visibility and justify the addressing of these
Techniques.

27. In an e-commerce firm, IT section is responsible for installing and configuring UiPath, which will be used to develop and deploy automation workflows for processing bills/invoices.
(i)Explain the basic system requirements needed for installing UiPath Studio, UiPath Robot and UiPath Orchestrator
(ii)Identify the correct order for the installation and activation of UiPath Studio, UiPath Robot, and UiPath Orchestrator for bills/invoice automation.
Step 1: Preparation.
Step 2: Install UiPath Orchestrator
Step 3: Install UiPath Robot
step 4: Install UiPath Studio
Step 5: Robot Configuration
Step 6: Activation and Configuration

28. Choose the appropriate justification for the given description
Description: -
1. LOIC (Low Orbit Ion Cannon)
2. Service unavailability, slow response, or complete downtime
3. Firewalls, rate limiting, IDS/IPS
4. DDoS (Distributed Denial of Service)

Justification: -
a) Helps detect, control, and block abnormal traffic
b) Uses multiple systems (botnets) to flood a target with traffic.
c) A popular DoS tool used to send massive requests and crash services
d) Prevents legitimate users from accessing critical online services.

29. The HR department of a MNC is seeking to automate the recruitment process using UiPath to ensure consistency, efficiency, and accuracy.
(i) Fill the design of an automated onboarding process in UiPath with proper justification. Also, explore the use of "Breakpoints" in debugging phase of UiPath.
1.Mapping the current process.
2. ___________
3. ___________
4. ___________
5. ___________
6.Monitoring and maintenance: Set up monitoring to ensure the automation runs smoothly and update it as necessary.

30. In a cloud-based dairy plant monitoring system, attackers can exploit XSS vulnerabilities in dashboard input fields, such as dairy processing data. Malicious scripts can steal user credentials, hijack sessions, or manipulate displayed sensor data.
Predict measures to prevent the following impacts.
I. Stealing user credentials
II. Hijacking sessions
III. Manipulating dairy processing data displayed on the dashboard