**Name :Sheharyar Khalid.**

**Task no 4**

**Topic:**

**Configuring Firewalls and Intrusion Detection Systems**

**Objective:**

* To protect the network by configuring firewalls and intrusion detection systems (IDS) to monitor and control network traffic, detect unauthorized access, and respond to potential threats.

**Steps to Implement:**

**1. Selecting Appropriate Firewall and IDS Solutions**

* **Firewall Types:**
  + **Network-based firewalls** (deployed at network boundaries, inspect traffic between networks)
  + **Host-based firewalls** (installed on individual devices, focus on incoming/outgoing traffic on that host)
  + **Next-Generation Firewalls (NGFW):** Include deep packet inspection, application-level inspection, and intrusion prevention systems (IPS) capabilities.
* **IDS/IPS Types:**
  + **Network Intrusion Detection Systems (NIDS):** Monitor traffic across entire networks.
  + **Host Intrusion Detection Systems (HIDS):** Monitor the specific host or device.
  + **Intrusion Prevention Systems (IPS):** Similar to IDS but also block the detected threats in real time.

**Key Considerations:**

* **Scalability:** Solutions should meet the needs of current and future network size.
* **Integration:** Ensure compatibility with other security solutions.
* **Performance:** Balance between thorough inspection and network latency.

**2. Configuring Firewall Rules and Policies**

* **Define security policies:**
  + Identify the assets needing protection and specify acceptable traffic.
  + Categorize network zones (e.g., trusted, untrusted, DMZ).
* **Set up inbound and outbound traffic rules:**
  + Block or allow traffic based on source/destination IP, port number, and protocol.
  + Use least privilege principle—allow only necessary traffic.
* **Best practices:**
  + Use a **default deny policy** for incoming traffic (deny all except necessary services).
  + Log dropped traffic for audit and analysis.
  + Enforce **stateful packet inspection (SPI)** to track traffic sessions.
  + Enable application-level inspection to block specific application-layer protocols.

**3. Setting Up IDS to Monitor Network Traffic**

* **Configure IDS/IPS:**
  + Place the IDS sensors in strategic network segments, such as:
    - Between internal network and the internet.
    - Near critical servers or data centers.
  + **Tuning signatures:** Regularly update and customize IDS signatures for known threats.
  + Set thresholds to minimize false positives and negatives.

**Network Traffic Monitoring:**

* Monitor key protocols (e.g., HTTP, HTTPS, DNS) and identify unusual patterns (e.g., excessive traffic to/from a specific IP).
* Use **heuristics or behavioral analysis** to detect anomalies.

**4. Analyzing IDS Alerts and Responding to Threats**

* **Incident Response Plan:**
  + Define a plan for investigating alerts and responding to incidents.
  + Categorize alerts based on severity (low, medium, high).
  + Automate alerting to send critical notifications to admins.
* **Common response actions:**
  + Block offending IPs or suspicious ports.
  + Quarantine infected systems.
  + Investigate logs to identify the source and scope of the attack.

**5. Regularly Updating and Maintaining Configurations**

* **Patch management:** Regularly update firewall and IDS software to address vulnerabilities.
* **Rule optimization:** Review and optimize firewall rules to remove unused or conflicting entries.
* **Signature updates:** Keep IDS signatures updated to detect emerging threats.
* **Periodic audits:** Perform regular security audits and testing, including penetration testing, to ensure the firewall and IDS configurations are functioning correctly.

**Maintenance Checklist:**

* Weekly: Review alerts and logs, apply signature updates.
* Monthly: Review and update firewall rules.
* Quarterly: Test IDS and firewall performance.
* Annually: Full audit of firewall and IDS systems.