1. Functional Testing in Cybersecurity

Purpose:

Ensures that security features in an application or system work as intended.

Key Areas of Functional Security Testing:

Authentication & Authorization Testing

- Verifies **Multi-Factor Authentication (MFA)** and **Role-Based Access Control (RBAC)**.
- Ensures unauthorized users cannot access restricted resources.

Vulnerability Testing

- Identifies **SQL Injection, Cross-Site Scripting (XSS), and security misconfigurations** using automated scanners (Nessus, OWASP ZAP).
- Validates **firewall rules, encryption protocols, and security headers**.

Penetration Testing

- Simulates **real-world attacks** to identify security loopholes.
- Tests **network security, APIs, and application security** against threats.

Data Security & Encryption Testing

- Ensures **TLS 1.2+, AES-256 encryption** is properly implemented.
- Verifies **data integrity** during storage and transmission.

Incident Response Testing

- Simulates **security breaches and ransomware attacks**.
- Evaluates **SOC & SIEM response efficiency** under attack scenarios.

Example Functional Test Scenario:

A tester attempts to log in with **brute-force attacks**, **invalid credentials**, or **bypasses authentication methods** to check if the system blocks unauthorized access.

---

2. Performance Testing in Cybersecurity

Purpose:

Evaluates how security mechanisms **perform under different conditions** to ensure they don't impact system efficiency.

Key Areas of Performance Security Testing:

Load Testing

- Measures **how firewalls, SIEMs, and authentication servers** perform under heavy traffic.
- Ensures DDoS protection mechanisms can handle large-scale attacks.

Stress Testing

- Simulates extreme conditions like **high login attempts, massive data transfers, or high-volume alerts in SIEM**.
- Ensures security components don't fail under stress.

Latency Testing

- Evaluates response time for **user authentication, encryption/decryption, and firewall processing**.
- Ensures minimal **latency in security services** like SIEM, IDS, and VPN authentication.

Scalability Testing

- Tests **how security systems scale with increased users, logs, and attack attempts**.
- Ensures SOC tools **can handle increased alerts and incidents** without failure.

Failover & Recovery Testing

- Simulates **server crashes, firewall failures, and SIEM outages**.
- Verifies if **backup security systems take over automatically**.

Example Performance Test Scenario:

A tester floods a **Web Application Firewall (WAF)** with 100,000+ requests per second to ensure it correctly detects and mitigates a **DDoS attack** without degrading system performance.