5. SYSTEM TESTING & IMPLEMENTATION

5.1 SYSTEM TESTING

In the system testing the whole system is tested for interface between each module and program units are tested and recorded. This testing is done with sample data. The securities, communication between interfaces are tested. System testing is actually a series of different tests whose primary purpose is to fully exercise the computer based system although each test has a different purpose all work to verify that all system elements properly integrated and perform allocate function.

In involves basic 6 kinds of activities namely

- Integration Testing
- Vulnerability Testing
- Configuration Testing
- Connectivity Testing
- Network Performance Testing

INTEGRATION TESTING

Integration testing verifies that individual network components, such as routers, switches, firewalls, and servers, work together as intended within the overall network architecture. It ensures seamless communication and interoperability between different elements of the network infrastructure.

Integration testing in the context of brute force attacks involves assessing how well different components of a system work together to defend against such attacks. It focuses on ensuring that various security mechanisms and controls, when integrated, effectively mitigate the risks posed by brute force attacks

Here's how integration testing can be conducted:

- Testing Authentication Mechanisms
- Testing Rate Limiting
- Testing Logging
- Testing Patch Management

VULNERABILITY TESTING

Vulnerability testing is an assessment used to evaluate application security by identifying, diagnosing, and triaging application vulnerabilities. The entire process requires application security (AppSec) teams to plan vulnerability tests and analyze results.

Vulnerability testing in the context of brute force attacks involves identifying weaknesses in a system that could be exploited by attackers attempting to gain unauthorized access through brute force methods

Here's how vulnerability testing can be conducted specifically for brute force attacks:

- Password Strength Assessment
- Credential Exposure Analysis
- Logging and Monitoring Analysis
-

CONFIGURATION TESTING

Configuration testing in a network involves assessing the settings, parameters, and configurations of network devices and components to ensure they are properly configured, secure, and optimized for performance.

Assess the configuration of firewall devices to ensure they effectively control traffic flow between network segments and enforce security policies. Test firewall rulesets to verify that only authorized traffic is permitted while unauthorized or malicious traffic is blocked. Ensure that default or unused rules are removed or disabled to minimize attack surface.

Configuration testing in the context of a brute force attack involves evaluating the settings, configurations, and security measures in place to defend against or mitigate the impact of such attacks.

If a Juniper router is subjected to a brute force attack, it means that unauthorized users are attempting to gain access to the router by repeatedly trying different username and password combinations until they find the correct ones. This could be extremely detrimental to the security and integrity of the network, as gaining access to the router could allow attackers to manipulate network settings, intercept traffic, or even bring down the network entirely.

NETWORK SECURITY TESTING

Security testing in a network, also known as network security testing, involves assessing the security posture of the network infrastructure to identify vulnerabilities, weaknesses, and potential threats. This helps organizations understand their security risks and take proactive measures to mitigate them.

Conducting vulnerability assessments involves scanning the network infrastructure to identify known vulnerabilities in systems, applications, and network devices

Security testing for brute force attacks involves evaluating the resilience of systems and applications against repeated login attempts aimed at guessing usernames and passwords.

Here's how security testing can be conducted specifically for brute force attacks:

- Password Policy Assessment
- Brute Force Simulation
- Monitoring and Alerting Testing

CONNECTIVITY TESTING

Connectivity testing in a network involves verifying that devices within the network can communicate with each other and access external resources as intended. This type of testing helps ensure that the network infrastructure is functioning correctly and that users can access the resources they need.

Ping is a simple network utility that sends ICMP (Internet Control Message Protocol) echo requests to a target device and waits for ICMP echo replies. Ping tests can be used to verify basic connectivity between two devices, assess network latency, and troubleshoot connectivity issues.

Connectivity testing in the context of a brute force attack involves assessing the ability of network services and resources to remain accessible and functional during an ongoing brute force attack.

By performing comprehensive connectivity testing in the context of a brute force attack, organizations can ensure that network services remain accessible and functional, even under sustained attack, while also enhancing their ability to detect, respond to, and recover from security incidents.

5.2 SYTSEM IMPLEMENTATION

Implementing a system to defend against brute force attacks involves deploying various security controls and mechanisms to detect, prevent, and mitigate unauthorized access attempts.

Strong Authentication Mechanisms: To defend against brute force attacks, put strong authentication mechanisms in place. This involves implementing multi-factor authentication (MFA), strict password policies, and, when appropriate, biometric authentication. It is more difficult for attackers to guess or use brute force login credentials when strong authentication is in place.

Web Application Firewalls (WAF): Install web application firewalls if necessary to defend against web applications being the target of brute force attacks. Before malicious login attempts are made, WAFs can examine incoming web traffic, spot suspicious requests, and either reject or block them before they reach the application backend.

Install a **Security Information and Event Management (SIEM)** solution to centrally store and correlate security events from a variety of sources, such as intrusion detection system logs, firewall logs, and authentication server logs. Real-time visibility into brute force attack attempts can be obtained by SIEM platforms, allowing for quick.

5.3 SYSTEM MAINTENANCE

Maintenance is actually implementation of the review plan as important as it is programmers and analyst is to perform or identify with him or herself with the maintenance

System maintenance for mitigating brute force attacks involves implementing proactive measures and regular upkeep to ensure the security, availability, and resilience of systems against such attacks.

Here's a comprehensive guide to system maintenance for brute force attack :

- **Regular Password Policy Review**
- **Network Security Controls**

REGULAR PASSWORD REVIEW

Conduct periodic reviews of password policies to ensure they align with industry best practices and security guidelines. Consider factors such as password length, complexity requirements, expiration periods, and account lockout thresholds.

NETWORK SECURITY CONTROLS

Regularly review and update network security controls, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and access control lists (ACLs), to block malicious traffic associated with brute force attacks. Implement rate limiting and throttling mechanisms to restrict the frequency of authentication attempts