IBA Institute of
Business Administration
Karachi

Leadership and Ideas for Tomorrow

Scope of Work

RFQ - 1533 - 5427-Vulnerability Assessment & Penetration Testing

Network Components:

- Identify and assess vulnerabilities in server network devices, including switches, routers, and firewalls.
- Evaluate the security configurations of network devices to ensure best practices are followed.
- Conduct penetration tests to identify potential weaknesses in the network infrastructure.

Firewall:

- Assess the effectiveness of the firewall configuration in preventing unauthorized access.
- Identify and test for potential vulnerabilities in the firewall rules.
- Evaluate the ability of the firewall to detect and block various types of attacks.

Routers:

- Review router configurations for security weaknesses.
- Test router access controls and authentication mechanisms.
- Evaluate the resilience of the routers against common network attacks.

Publicly Accessible Web Servers:

- Conduct a thorough assessment of publicly accessible web servers for vulnerabilities.
- Test web server configurations, including SSL/TLS settings.
- Evaluate the security of web applications hosted on these servers.

Documentation and Reporting:

- Provide a detailed report outlining discovered vulnerabilities, their severity, and recommended remediation steps.
- Include an executive summary for non-technical stakeholders.
- Provide evidence of successful penetrations where applicable.

Rules of Engagement:

- Specify the testing window and any blackout periods.
- Define the extent to which penetration testing can be conducted (e.g., testing without causing service disruptions).
- Identify any restricted areas that should not be tested.

Legal and Compliance Considerations:

- Ensure that all testing activities comply with applicable laws and regulations.
- Obtain necessary permissions from the organization's legal and compliance teams.

Communication:

- Establish clear communication channels for reporting findings and progress.
- Define contact points for incident response in case unexpected issues arise.

Post-Testing Support:

- Provide support and clarification regarding identified vulnerabilities.
- Assist in the implementation of recommended remediation measures.

Bill of Quantity

Devices	Qty
Routers	3
Core Switches	2
Firewalls	2
Physical hardware	6
Server VMs	10
Databases Instances	6