Vulnerability and Pen Testing Activity Scope of work.

This is the scope of work for the threat Risk Assessment and Vulnerability Analysis for the sole reason for distinguishing classifying and mitigation of any risk found during the assessment. To viably assess and evaluate the security measures and recognize all risks to the security of information as a result of the architecture and the configuration of the infrastructure implemented. This assessment requires a certain and detailed rundown of vulnerabilities and suggested mitigations for the risks associated with each of them. And that are twenty-Three assets in which windows servers, firewalls, routers and switches are included. Assessments based on World's top five best standard tools and methodologies i.e., Nexpose VA, OWASP, Zen Map and security reviews. High level test cases.

- Internal Network Scanning
- Port Scanning, Discovery
- enumerate information
- Check for anonymous SMB shares
- Check for open NFS shares
- Check for anonymous FTP shares
- Identify all URLs that allow logins
- MITM attacks
- Traceroute Information

1. Internal vulnerability assessment and penetration Testing reconnaissance, Vulnerability assessment, Exploitation of all internal services using well known audit tools 7 IP addresses.
2. External Vulnerability assessment and Penetration testing Reconnaissance, Vulnerability Assessment, Exploitation of all External Services using well know audit tools 2 IP address
3. Reporting in depth reporting of the results taken from both external and internal services 14 IP address.
4. The objective of this assignment will be to identify the risks posed to IBA's IT environment and recommendations to mitigate the identified risks. Following will be achieved out of this project.
5. Access the security posture of their existing IT Infrastructure.
6. Identify the security loop holes as per the scope.
7. Implement the work around where necessary, to close the identified security gaps. To find out the vulnerabilities in IBAs network and take proactive measures before it gets compromised.

BOQ

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