ISLAMI BANK BANGLADESH LIMITED

OPERAIONS WING, ENGINEERING DIVISION
PROCUREMENT OF COMPUTER HARDWARE
AND ACCESSORIES DEPARTMENT
20, DILKUSHA C/A (9th Floor), DHAKA – 1000.

Notice for procurement of Penetration Testing Tools for Islami Bank Bangladesh Limited.

Sealed Tenders are hereby invited by Islami Bank Bangladesh Limited from Authorized Companies / Local Agents / Dealers / Distributors for procurement of Penetration Testing Tools for Islami Bank Bangladesh Limited under the following terms and conditions:

Brief specification of the items is as under:

Specification of the Penetration Testing Tools

Sl. No.	Item description	Item Details
1	Penetration Testing Tools	One (1) Named User Perpetual License (Unlimited IP)

Technical Specification / Requirement

The Mandatory (M) and Desired (D) technical specifications are given below –

Item	Question / Requirement	Bidder Response
1.	What are recommended system requirements to operate the solution?	
2.	What is the average time for implementation?	
	Solution Requirements: Interface	
Item	Question / Requirement	Bidder Response
3.	The solution must supply the following methods of user interaction:	
	✓ Wizard-based test setup and configuration	
	✓ Automated exploit selection and execution	
	✓ Ability to select and run individual exploits	
	✓ Ability to schedule tests	
	✓ Ability to create custom testing workflows	
	✓ Ability to customize the solution and exploits	
	✓ Ability to write and run our own exploits using the solution	

Solution Requirements: Network Penetration Testing		
Item	Question / Requirement	Bidder Response
4.	The solution must be able to automatically identify and profile network systems given a specific IP range.	
5.	The solution must provide a variety of network discovery and port scanning methods.	
6.	The solution must be able to import results from multiple network vulnerability scanners and validate the results for exploitability.	
7.	The solution must be able to target and test systems running operating systems including Windows, Linux, Mac, AIX, Sun Solaris and OpenBSD.	
8.	Solution must be able to interact with different databases.	
9.	How many exploits are currently included with the solution's exploit library? Which library they use on exploit?	
10.	New exploits and other updates should be available on a frequent basis.	
11.	The solution's exploits must be customizable.	
12.	Exploit payloads must have a minimal footprint on tested systems.	
13.	Exploit payloads must provide an interface to systems compromised during testing to determine the implications of a breach.	
14.	Exploit payloads must provide access to system calls and Windows APIs.	
15.	Exploit payloads must support binary plug-ins and code.	
16.	Exploit payloads must support multiple connection methods.	
17.	Payloads must not be vulnerable to take over or MiTM (Man in The Middle) attacks that turn the payload into a backdoor.	
18.	Communication between the testing platform and all payloads must be encrypted to prevent loss of data via sniffing.	
19.	The solution must be able to maintain contact with compromised systems that are restarted.	

20.	The solution must include capabilities to assess the ability of attackers to gain administrative privileges on compromised systems.	
21.	The solution must be able to pivot between target systems to replicate an attacker's attempts to move through the network.	
22.	The solution must be able to run third-party applications against systems compromised during testing	
23.	The solution must ensure that no code is left behind on tested systems.	
24.	The solution must minimize the amount of files written to disk at the target systems.	
25.	The solution must be able to leverage weak or default credentials to gain access to target systems.	
26.	The solution must offer a closed loop method to determine the strength of windows passwords based on discovered hashes.	
27.	The solution must be able to test Surveillance Cameras.	
28.	The solution must be able to re-test vulnerabilities previously found.	
29.	The solution must include capabilities multiple attack vectors to be performed against the same network.	
30.	The solution must allow the user to replicate multi-staged attacks that can pivot across devices and applications	

Solution Requirements: Web Application Penetration Testing		
Item	Question / Requirement	Bidder Response
31.	The solution must have automated web crawling capabilities to identify pages to test in web applications.	
32.	The solution must support a wide range of authentication methods.	
33.	The solution must be able to discover web applications in hosts running HTTP servers.	
34.	The solution must be able to import results from multiple Web Applications vulnerability scanners and validate the results for exploitability.	

35.	The solution must be able to evaluate JavaScript for vulnerabilities.	
36.	The solution must include capabilities for testing OWASP Top 10 web applications vulnerabilities, including Cross-Site Scripting (XSS) and SQL Injection. Please list all penetration testing capabilities for OWASP Top 10 vulnerabilities.	
37.	The solution must test for exploitable Local and Remote File Inclusion vulnerabilities.	
38.	The solution must test for exploitable Cross-Site Scripting vulnerabilities in Adobe Flash objects.	
39.	The solution's web application penetration testing capabilities must enable testers to assess the implications of a web application breach, such as identifying the data exposed by a vulnerability and / or conducted a subsequent attack against the backend network.	
40.	The solution must be able to detect and check Web Services for vulnerabilities.	
41.	The solution must be able to re-test vulnerabilities previously found	
	Solution Requirements: Client-Side Penetration Testing	
Item	Question / Requirement	Bidder Response
42.	The solution must include automated capabilities for gathering email addresses and other publically available information to be used in penetration tests.	
43.	The solution must have the ability to test the exploitability of vulnerabilities in many common client applications.	
44.	The solution must be able to replicate attacks stemming from malicious email attachments or originating from flash drives.	
45.	The solution must be able to replicate phishing attacks that redirect end-users to web servers hosting malicious content and/or serving as imposters of legitimate web sites to assess data leakage issues.	
46.	The solution must include capabilities to conduct phishing awareness tests without exploiting end-user systems.	
47.	The solution must enable testers to determine if an end-user system compromised by a client-side attack exposes other systems on the same network to subsequent attacks.	
	Solution Requirements: Wireless Network Penetration Testing	
Item	Question / Requirement	Bidder Response
48.	The solution must include capabilities for discovering and analyzing wireless networks.	

49.	The solution must assess the exploitability of networks encrypted with WEP, WPA and WPA-2.	
50.	The solution must be able to replicate wireless man in the middle attacks.	
51.	The solution must be able to detect systems probing for SSIDs.	
52.	The solution must be able to impersonate SSIDs (karma).	
Solution Requirements: Mobile Device Penetration Testing		
Item	Question / Requirement	Bidder Response
53.	The solution must include capabilities for demonstrating the exploitability of smartphones. (Please mention the solution's smartphone testing capabilities, including target mobile platforms.)	
54.	The solution must offer multiple smart phone attack replication capabilities. (Please describe each mobile device attack capability.)	
55.	The solution must demonstrate exploitability through evidence retrieval capabilities. (Please describe all evidence retrieval capabilities included in the solution.)	
56.	The solution must allow use to interact with the compromised device.	

Training		
Item	Question / Requirement	Bidder Response
57.	Describe training options for the solution.	
58.	Describe instructor-led training options for the solution.	

Detail specification is mentioned in the Tender document.

Terms and Conditions:

01. The intending Bidders have to apply in their letter head pad and must submit documentary evidence like VAT registration Certificate, Trade License, Authorized certificate for delivering of the item in support of their past experience and specialization in the field. On being satisfied with documents submitted by the applicant, Tender document will be sold to the intending bidders from Procurement of Computer Hardware and Accessories Department, ED, HO, IBBL, 20 Dilkusha, Yousuf Chamber (9th floor) during Office hours from **29.03.2018 to 17.04.2018** upon payment of **Tk.5,000.00 in cash (non refundable)**. No Tender document will be issued/ received by mail.

02. Tenders will be received at the office of the undersigned up to **2.30 P.M on 18.04.2018** and only Technical offers will be opened at **2.40 P.M** on the same date and same place that is in the office of the undersigned in presence of the bidders who may like to attend to the tender opening meeting. After completion of technical evaluation, financial offer of the technically qualified bidders will be opened through informing the same to the participating bidders.

03. Tk.1,00,000.00 (Taka one lac only) must be submitted along with the technical offer of the tender in favour of Islami Bank Bangladesh Limited in the form of Bank Draft/ Pay Order/ Bank guarantee from any scheduled Bank of Bangladesh preferably from Islami Bank Bangladesh Limited without which the Tender shall be rejected outright. The Bank Guarantee must be valid for 6 (six) months primarily and after issuing of work order, the BG should be validated until the successful completion of awarded works.

04. An original and one copy of the Offer duly marking **"Original Offer_Technical''** and **"Copy of the Offer_Technical"** and **"Original Offer_Financial'' and "Copy of the Offer_Financial"** should be submitted at the time of tender submission with authentication by the Tenderers. **Combination of Technical and Financial Offer will be disqualified.** The bid form must be filled in through computer printer or in typing without overwriting and without any erasing and modifications and when completed shall contain all the required information.

05. Islami Bank Bangladesh Limited reserves the right to accept any tender and reject any or all tenders without assigning any reason whatsoever. Islami Bank Bangladesh Limited is not bound to purchase the item from the lowest bidder.

06. The offered solution by the bidders must meet all of the above given technical specification outlined in the tender. Any deviation would be considered disqualification of the solution to be offered.

Senior Vice President