Bid Notice Abstract

Request for Quotation (RFQ)

Reference Number	6710271
Procuring Entity	ANTI-MONEY LAUNDERING COUNCIL
Title	Penetration Testing Tool
Area of Delivery	Metro Manila

Printable Version

Solicitation Number:	PR No. 19-050
Trade Agreement:	Implementing Rules and Regulations
Procurement Mode:	Negotiated Procurement - Two Failed Biddings (Sec. 53.1)
Classification:	Goods
Category:	Information Technology
Approved Budget for the Contract:	PHP 1,340,000.00
Delivery Period:	45 Day/s
Client Agency:	
Contact Person:	CONRAD DICDICAN BULANADI Bank Officer II Rm 612, 6/F EDPC Bldg., BSP Complex Malate, Manila Manila Metro Manila Philippines 1004 63-2-3023848 63-2-7087909 cbulanadi@amlc.gov.ph

Status	**Active**
Associated Components	Order
Bid Supplements	0
Document Request List	1
Date Published	29/11/2019
Last Updated / Time	29/11/2019 12:00 AM
Closing Date / Time	06/12/2019 1:00 PM

Description
AMLC BIDS AND AWARDS COMMITTEE

REQUEST FOR QUOTATION

The AMLC Secretariat will undertake a Negotiated Procurement for the "Penetration Testing Tool" in accordance with Section 53.1 of the Implementing rules and Regulations of Republic Act No. 9184.

Name of the Requirement/Brief Description: "Penetration Testing Tool"
Specifications:

Installation, Deployment and Integration
• Solution must be able to support installation on 64-bit Linux and Windows (64-bit).
• Solution shall have latest updates (e.g. exploit module) as frequent as on a weekly basis.
• Solution shall support offline activation and manual updates.
• Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.

Administration
• Solution must include web-based user interface through encrypted channels.
• Solution shall support command line console within.
• Solution shall allow API integration with other systems or be able to automate workflow.
• Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.

Host Scan and Web Scan
• Solution shall conduct scans and discover the host's OS and running services.
• Solution shall support customized nmap command for scan.
• Solution shall support dry runs to show the scan information in task log only.
• Solution must be able to integrate with other pentest tool to discover host's OS, running services and vulnerabilities via existing scan results or new scans.
• Solution shall support automatic tag by OS where applicable.
• Solution must support importing of scan result from external solutions including but not limited to Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact.

System Exploitation
• Solution shall be able to apply exploits on individual IP or multiple IPs.
• Solution shall automatically select and apply exploit modules based on OS, service and vulnerability references.
• Solution shall have at least 6 reliability levels of exploit codes for automated exploitation.
• Solution shall support running individual exploit module manually from the user interface.
• Solution shall support dry run to show exploit information in task log only.
• Solution shall support replay of exploitation tasks.
• Solution shall support automation of common yet complicated security tests (Metamodules) that provide a more efficient way to get specific jobs done.
• Solution shall support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network.

Bruteforcing
• Solution shall support bruteforce testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM.
• Solution shall provide password references for factory default logins.
• Solution shall support customized credentials and dictionary import for bruteforce.
• Solution shall support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.

Post Exploitation Action and Evidence Collection
• Solution must support exploitation payload types "Meterpreter", "Command Shell" and "Powershell".
• Solution must support customized macros to run selected operations automatically after exploit.
• Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.
• Solution must support deploying of persistent listeners to allow exploited hosts to connect back to Metasploit automatically.

Social Engineering Campaign

• Solution must support web campaign, Email campaign and USB campaign.
• Solution must allow web campaign customized with http/https, IP address, port and path (e.g. https://www.abc.com:1234/abcd).
• Solution must support web content to be cloned from another web site (e.g. www.google.com).
• Solution must support web campaign that browser autopwn (apply all the appropriate exploit modules based on the browser version), specific browser exploit (e.g. MS11-050) and not do anything (just checking the connection from the users).
• Solution must support email campaign content customization to include a specific URL or an agent attachment.
• Solution must support USB campaign that generates an agent deployment .exe file.

Web Application Exploitation
• Solution must support web crawling on IPv4 and IPv6 web sites.
• Solution must support web crawling applied on a web site (e.g. http://www.abc.com) or started from a specific point (e.g. http://www.abc.com/path/starthere/).
• Solution must support detection of vulnerable URLs and parameters such as SQL Injection and Cross Site Scripting.

Report and Data Export
• Solution must provide built-in standard reports and support customized report functionality.
• Solution must provide built-in standard reports.
• Solution must support report formats including but not limited to PDF, Word, RTF and HTML.
• Solution must support reports to be stored locally and sent to recipient by email after created.
• Solution must be able to support data export which allows a zip archive of the project suitable for importing into an another instance of the solution.

Global Recognition
• Solution must be market leading and/or highly rated (by a third-party review company such as Gartner, Forrester, NSS Labs, etc.) ICT Security System.
• Solution must be existent in the Philippines for at least five (5) years.

Supplier Experience/Qualifications
• The supplier must have supplied and deployed PenTest Tool for the last three (3) years.
• The supplier must have technical support engineers, who are regular, locally based and experienced personnel to be assigned with the PenTest Tool project.
• The supplier must have undergone training and has certification of completion of deployment and management of PenTest Tool.
• The supplier must have professional project manager who are regular, locally based and experienced personnel to be assigned with this project.
• The supplier must have local helpdesk facility and system that accepts cases and monitors the progress of each open case incident.
• The supplier must have experienced and trained technical staff or engineers under its direct employment to render help desk assistance or support.

Maintenance and Support
• One Year Maintenance & Software Subscription for Pentest Tool (Software) with One Year Annual Maintenance - Version Releases, Patches, and Unlimited Phone and Email Support to service provider.
• One Year Local Standard Technical Support - Provide unlimited phone and email support during normal business
• The supplier must provide a grace period for the license renewal of sixty (60) calendar days from the date of expiration of software maintenance.

Knowledge Transfer
• The supplier should provide knowledge transfer for at least nine (9) ESS personnel.
• A certificate of training must be issued by the supplier to each seminar attendee upon completion of the knowledge transfer.

Other Requirements
• Total Cost includes 12% VAT
• Bid Validity: 45 calendar days

Approved Budget for the Contract: Php1,340,000.00
Delivery/Completion 45 calendar days after receipt of Purchase Order

All particulars and activities relative to the eligibility of bidders/suppliers, Preliminary Meeting (if applicable), Evaluation of Bids and Award of Contract shall be governed by Republic Act No. 9184 and its 2016 Revised Implementing Rules and Regulations.

Interested suppliers are required to submit their PhilGEPS Certificate of Registration and price quotation (Annex "A") on or before 01:00 p.m. of 6 December 2019.

The Lowest Calculated Bidder shall submit, within five (5) calendar days upon receipt of notice from this Office, the following documents:

Legal Documents:
1. Y2019 Mayor's/Business Permit;
2. Income/Business Tax Return; and
3. Omnibus Sworn Statement.

The AMLC Secretariat assumes no responsibility whatsoever to compensate or indemnify any bidder/supplier for expenses incurred in the preparation of the bid/quotation.

The AMLC Secretariat reserves the right to reject the financial proposal or not award the contract and makes no assurance that a Contract shall be entered into as a result of this request.

Created by	CONRAD DICDICAN BULANADI
Date Created	28/11/2019

Back