Πειραιάς, 02/12/2024

PROVISION OF TENDER CLARIFICATIONS / EXTENSION

Subject: PROVISION OF VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) SERVICES ON IT SYSTEMS

The interested parties are kindly requested to refer to all the clarifications and any additional information published by PPA S.A. regarding the present tender. Therefore, please visit PPA S.A.'s website regularly to be informed about the latest information concerning the present tender.

The present reply constitutes an integral part of the Call

Question 10

"……..10.1. Could you please clarify if revalidation is mandatory for all of respective PTs in scope?....."

"……..10.2. Each item in scope of the project (page 10of RFP) can be addressed as distinctive 11 δια PTs (11) or they can be grouped per category. For example, 1 External Black Box PT, 1 Internal PT, etc? ....."

Answer 10:

10.1 Full retesting is not mandatory, but PPA may, at its discretion, request a retesting for individual findings.
10.2 The items in the scope can be grouped per category, provided the methodology ensures comprehensive coverage as per the tender specifications.

Question 11 External Black Box Penetration Scan

"……. 11.1. Please provide us with the approximate number of live public IP addresses to be considered in scope....."

"……. 11.2. How the Penetration Testing will be performed in terms of attacker's knowledge regarding the scope?
a. Zero Knowledge (only the target company name will be provided).
b. Specific network ranges will be provided (network discovery required).
c. Specific IP addresses will be provided. ....."

Answer 11:

11.1 External infrastructure components are included in the tender under "Public Applications" and "External Network Components".
11.2 The External Black Box Testing will be conducted with no prior knowledge of the infrastructure.
Grey Box VAPT services must be provided for all items in the scope as per the tender specifications.

Question 12 Internal Penetration Scan

"……. 12.1. How the Penetration Testing will be performed in terms of attacker's knowledge regarding the scope?
a. Zero knowledge.
b. Specific network ranges will be provided (network discovery required).
c. Specific IP addresses will be provided....."

Answer 12:

Specific IP addresses will be provided.

Question 13

"……. 13.1. Is an additional attack scenario that involves knowledge of domain credentials required?*Focused on Active Directory attack vectors……"

Answer 13:

Yes, scenarios involving domain credentials are included in the scope. Detailed technical descriptions will be provided to the selected bidder during the project initiation phase.

Question 14

"……. 14.1 How the Penetration Testing will be performed in terms of attacker's positioning?
a. Full network visibility (e.g. admin network, any/any)
b. Limited network visibility (e.g. back office, guest network) ……"

Answer 14:

Network visibility will be confirmed with the selected bidder during the project initiation phase.

Question 15

"……. 15.1. Could you please provide us the number of different site facilities, where the above SSIDs are located ?……"

Answer 15:

One Site.

Question 16

"……. 16.1. Which of the below activities are considered in scope for the engagement?
a. Simulation of an attacker located within physical range and attempts (i) to obtain unauthorized access to the wireless network and (ii) perform man-in-the-middle attacks to the connected clients (rogue access point).
b. Simulation of an attacker that has already knowledge of wireless credentials (guest network/corporate network) and targets the accessible corporate infrastructure (Network Penetration Test).
c. Validation of the network segregation (e.g. unauthorized access to the corporate network through the guest network) assuming knowledge of wireless credentials. ……"

Answer 16:

All above activities. Technical details will be confirmed with the selected bidder during the project initiation phase

Question 17

"……. 17.1. In case an infrastructure level penetration test of all components of the network is also required (Network Penetration Test), please provide with an approximate number of the internal systems in scope……"

Answer 17:

A total of 4 internal network components (IP addresses)

Question 18

"……. 18.1.1 Please provide a brief description of the applications usage and purpose

18.1.2. Please provide us the applications names.

18.1.3. How the application in scope will be accessed for testing?
a. Application is publicly accessible.
b. Remote access will be provided (e.g VPN).
c. Onsite presence required.

18.1.4. Please provide us the approximate number of application's dynamic web pages

18.1.5. Please provide the number of different application roles that need to be tested (e.g. regular user, operator, etc.)

18.1.6. In case the application uses web services to exchange information, please inform us about the approximate number of calls in scope.

18.1.7. Do the applications include a Multi-Factor Authentication (MFA) mechanism?

18.1.8. Do the applications include a self-registration functionality?

18.1.9. Does the application include an online trading/e-commerce functionality (financial transactions)?

18.1.10. In case the application in scope is built/based on a commercial or open-source CMS (e.g. Wordpress, Joomla, Drupal etc.), WMS (e.g. Liferay), ECM (e.g. Sharepoint) or any other platform, please provide us the platform name

18.1.11. In case the scope includes a thick client (desktop application), please specify the communication protocol(s) with the server-side part……"

Answer 18:
Detailed technical descriptions of the applications, including access methods, features, and configurations, will be provided to the selected bidder during the project initiation phase.
On-site presence is not required for tasks that can be performed remotely and a VPN access to jumphost will be provided.

Question 19
"……. 19.1. Endpoint Security Configuration Audit: Is any EDR solution used on endpoints? If yes, kindly provide us with the respective solution brand name……"

"……. 19.2. Endpoint Security Configuration Audit: Is an approach including tool-driven execution of the compliance authenticated scans against CIS benchmarks sufficient?……"

Answer 19:
19.1 An EDR solution is implemented. Technical descriptions EDR will be provided to the selected bidder during the project initiation phase.
19.2 Tool-driven execution of compliance authenticated scans against CIS benchmarks is acceptable.

Question 20
"……. 20.1. Server Security Configuration Audit: Is any EDR solution used on servers? If yes, kindly provide us with the respective solution brand name……"

"……. 20.2. Server Security Configuration Audit: Is an approach including tool-driven execution of the compliance authenticated scans against CIS benchmarks sufficient?……"

Answer 20:
20.1 An EDR solution is implemented. Technical descriptions EDR will be provided to the selected bidder during the project initiation phase.
20.2 Tool-driven execution of compliance authenticated scans against CIS benchmarks is acceptable.

Question 21
"……. Kindly clarify whether retesting activities will be required after the completion of the initial penetration testing activities……"

Answer 21:
Full retesting is not mandatory, but PPA may, at its discretion, request a retesting for individual findings.

Question 22
"……. regarding the requested service of Configuration Audit, we would like to request the following clarifications in order to proceed to an accurate sizing of the project.
23.1. Operating System and its version (of both the servers and the workstations).
23.2. List of name and version of each additional software that needs to be assessed on each device. ……"

Answer 22:
Detailed technical descriptions of operating systems and software versions will be provided to the selected bidder during the project initiation phase.

Question 23
"……. 23.1. Applications (both Public & Internal): Please define the type of applications (e.g. web ppplications).
"…….23.2. Please clarify whether authenticated assessments will be performed.
"……. 23.3. Please define the size of the applications (Number of forms, Api calls, Roles, etc)……"

Answer 23:
Detailed technical descriptions of the applications will be provided to the selected bidder during the project initiation phase.

Question 24
"……. 24.1. **Critical Systems:** Is Active directory included in the scope of the assessment?……"

Answer 24:
Yes

Please be informed that an extension of the tender's deadline is granted until Friday 06.12.2024 16:30 Greek time (GMT +2)