**Penetration testing requirements**

**General Scope**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Stage of work** | **Stage Description** | **Results** |
| 1 | Preparatory phase | Formulation of goals, objectives and scope of work | The works on modeling of targeted attacks.  A report has been prepared containing a systematization of possible attack scenarios and vulnerabilities, as well as recommendations for improving the level of security.    A workshop for the Blue Team was held and a report was prepared for senior management. |
| Harmonization of restrictions |
| 2 | Cyber intelligence and development scenarios | Cyber intelligence |
| Developing an attack scenario map |
| Matching the 3 most probable attack scenarios |
| 3 | Scenario Modeling and Testing | Scenario modeling |
| Adaptation of scenarios to research conditions and initial verification |
| Testing scenarios and execution of the attack |
| 4 | Final phase | Preparing a technical report on attack scenarios |
| Preparation and presentation of the report |
| Workshop for employees of the information security department |
| Preparation of a report for top management |

**Penetration Testing Methodologies and Standards**

The Vendor shall provide automated, manual or hybrid penetration testing Services, as requested. Clients may request the Vendor to perform various types of penetration testing Services such as White Box, Black Box or Grey Box testing.

The Vendor shall provide penetration test Services following appropriate industry wide, highly recognized methodologies and standards such as:

* Open Source Security Testing Methodology Manual (“OSSTMM”).
* National Institute of Standards and Technology (“NIST”).
* Open Web Application Security Project (“OWASP”).
* Penetration Testing Execution Standard (“PTES”).
* Payment Card Industry (“PCI”) Data Security Standard (“DSS”) Guidance: PCI Information Supplement.
* Federal Risk and Authorization Management Program (“Fed RAMP”).
* Information Systems Security Assessment Framework (ISSAF).
* British Standards Institution (BSI) Penetration Testing Model.
* Web Application Security Consortium (WASC) Threat Classification.

**General Requirements on Penetration Testing Services**

* Establish an incident and escalation management process to handle issues that may happen during the test.
* Identify information to be provided by Client based on the nature of test being performed (e.g., White Box, Black Box, GreyBox).
* Identify targets and map attack vectors.
* Identify the exploitable vulnerabilities.
* Exploitation (e.g., elevating privileges) within the scope.
* Provide reporting to Client as further stated.

**Penetration Testing Services Clean Up**

The Vendor shall clean up properly after penetration testing Services completion ensuring Client’s environments are not impacted as a result of the penetration testing Services, the cleanup activities include but are not limited to the following:

* Update and/or removal of test accounts added or modified during testing.
* Update and/or removal of database entries added or modified during testing.
* Uninstall test tools or other artefacts as applicable.
* Restoring security controls that have been altered for testing.
* Provide Clients with necessary information and/or guidance on how to verify Client’s environments have been restored.
* Provide Client with confirmation that the environments have been cleaned and restored.

**Penetration Testing Services Reporting and Presentation**

The Vendor shall provide Client with a report for each Service completed, the report shall include the following information at a minimum:

* Executive Summary.
* Scope of Services.
* Identification of critical components and explanation of why these components were tested.
* Methodologies and tools used to conduct the testing.
* Any constraints that impacted the testing (e.g., specific testing hours, bandwidth, special requirements).
* Description of the progression of the test and issues encountered during the testing with timelines.
* Findings from the tests (e.g., exploitation, severity) with details.
* Affected targets in Client’s environments.
* Recommendation on remediation.

**Selection Criteria**

Candidate should provide documentation at VTB Bank Georgia’s head office in sealed envelopes, on the following address: 14, G. Chanturia St., 0108.

**Following documentation is required to be submitted in paper form:**

* Experience in penetration testing (financial sector):
  + Candidate should have at least 5 years of experience in relevant field and should provide short description, scale and number of implemented penetration testing projects.
  + Minimum one recommendation letter about successful implementation of similar project in financial sector (would be a plus).
* Project timeline (by each scope) and completion time.
* Total price of the project.
* Price breakdown by each scope.
* Evaluator should have permanent staff of experts with relevant certification (CISA, OSCP, OSWE, OSCE, OSEE, SANS GIAC, LPT (Master), GXPN, ECSA (Practical), GMOB, etc..) and provide number of certified personnel.

For additional information, contact us on the following e-mail: [**d.pruidze@vtb.ge**](mailto:d.pruidze@vtb.ge)**,** [**k.khutsurauli@vtb.ge**](mailto:k.khutsurauli@vtb.ge)

Candidates will be selected based on the following variables:

* Ability to meet the requirements.
* Experience in relevant field.
* Price (must be fixed cost).