بسم الله الرحمن الرحيم

Ministry of Climate Change, Environment and Energy
Republic of Maldives

DIGITAL MALDIVES FOR ADAPTATION, DECENTRALIZATION AND DIVERSIFICATION (D'MADD) PROJECT
P177040

TERMS OF REFERENCE

for

Hiring of an Individual consultant for system penetration testing (National)

Reference No: MV-MoECCT-DMADD-361688-CS-INDV

Issued on:
03/26/2024

Advertisement No.:
(IUL)438-DMADD/438/2024/130

1. INTRODUCTION

The Digital Maldives for Adaptation, Decentralization and Diversification (D'MADD) Project (P177040), aims to support the Maldives in its digital transformation. The D'MADD project is funded by a grant from the World Bank and is implemented by the Ministry of Climate Change, Environment and Energy (MoCCEE). The key stakeholders include the National Centre for Information Technology (NCIT), the Communications Authority of Maldives (CAM) and the Department of National Registration (DNR).

The project will assist the government in laying the legal and regulatory foundations for the digital economy and the provision of digital services, fostering the growth of high-quality and reasonably priced Internet services, and fostering trust in digital transactions and service delivery. Hence, the project will fund technical assistance to strengthen legal and regulatory frameworks in such areas as data protection, cybersecurity and cybercrime, electronic transactions, and identification, and provide support for their operationalization through enhancing institutional capacity and developing pertinent roadmaps, strategies, and other tools and guidance.

The Project aims to support the use of digital technologies to decentralize, diversify and to adapt to climate change. The project objective is to enhance the enabling environment for the digital economy in Maldives, to improve identification for in-person and remote service delivery, and to leverage data and analytics for a green, resilient, and inclusive development. It is designed around three components and the proposed activities are conceived following the country's priorities and funding needs in the medium term. The components are as follows:

Component 1: Enabling environment for improved digital connectivity and competitiveness

1.1. Improving regulatory frameworks, oversight, and enforcement for a competitive broadband market

1.2. Empowering public institutions for digital transformation in Government

Component 2: Digital identification for improved online and in-person service delivery

2.1. Legal and institutional enablers and safeguards for secure data and identity management

2.2. Modernizing of the foundational ID system and credential

2.3. Strengthening the digital authentication ecosystem

Component 3: Digital technologies and data platform for climate resilience

3.1. Establishing a climate data platform

3.2. Leveraging digital technologies and tools for climate adaptation

2. BACKGROUND

The Department of National Registration (DNR) under the Ministry of Homeland Security and Technology is mandated to establish a civil registration system, to formulate standards for maintaining record keeping of civil population and maintain official civil registration. The process was computerised in 2003. The National Registration, Identification and Verification System (NRIVS) is designed to maintain the history of citizen information from birth to death. DNR shares identity-related data in certain authorized contexts with multiple government organizations via APIs on the National Computer Network (NCN) operated by the NCIT.

DNR requires the services of an Individual consultant to conduct penetration testing of its Information Systems and Infrastructure.

The ToR will support the implementation of subcomponent 2.2(a) of the D'MADD Project, "The modernization of the foundational ID system and credential" and will support the design and implementation approach of proposed future upgrades for the NRIVS.

3. OBJECTIVE

The objective of this assignment is to engage a qualified entity to conduct a comprehensive penetration testing exercise to identify the security posture of DNR's network infrastructure, systems, and applications. The assessment will involve conducting simulated attacks, identifying vulnerabilities, and providing detailed reports on the findings, including recommendations for remediation. The primary goal is to enhance the overall security posture and resilience of DNR's digital assets by addressing potential weaknesses and strengthening defensive measures.

4. SCOPE OF THE ASSIGNMENT

The following scope of assignment outlines in general, the activities and responsibilities expected from the consultant to successfully achieve the stated deliverables in section 5.

4.1. Carry out pre-assessment discussions with DNR and define a plan with clear objectives and the scope of boundaries. The Coverage areas of the Vulnerability Assessment and Penetration Testing (VAPT) Plan are provided in ANNEX 1. The Consultant shall consider the business of the organization while planning the testing and vulnerabilities and ensure they are prioritized in accordance with DNR and feedback. The Plan and Methodology must obtain clearance and acceptance by DNR prior to implementation. The plan should cover precautionary measures to be taken, planning, test matrices, approach, and methodology in the presence of the technical team and representatives from the management team. As such, the plan should include, but not limited to the following.

4.1.1. Scope of the VAPT activity.

4.1.2. Timeline.

4.1.3. Resources i.e, Individual authorized to conduct the assessment along with their credentials.

4.1.4. Tools to be deployed/used.

4.1.5. Assurance of zero risk / restoration.

4.1.6. Assessment's logistics (details of places & IP addresses for external & covert tests).

4.1.7. Handling of sensitive/critical data and servers.

4.1.8. Business Continuity Plan (BCP) and Operational impact.

4.1.9. Measures to be taken in the event of an incident.

4.1.10. Immediate mitigation measures in case of unseen disruption of services.

4.2. The consultant must use comprehensive approaches (such as Vulnerability Assessment via White Box, Black Box and Gray Box Testing and Penetration Testing with Red Team Attack Simulation) that combine various types of penetration testing, social engineering, and physical security assessments to simulate a real-world attack scenario and test an organization's overall security posture and incident response capabilities. As such the consultant must cover the following scope.

4.2.1. Network Penetration Testing to evaluate the security of network infrastructure, including firewalls, routers, switches, and other network devices, to identify vulnerabilities and potential entry points for attackers.

4.2.2. Web Application Penetration Testing to assess the security of web applications, including websites and web services, to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and authentication flaws.

4.2.3. Wireless Network Penetration Testing to examine the security of wireless networks, including Wi-Fi networks, to identify vulnerabilities and potential security weaknesses that could lead to unauthorized access or data leakage.

4.2.4. Social Engineering exercises simulating human-based attacks to assess an organization's staff awareness and susceptibility to phishing attacks, pretexting, or other forms of manipulation.

4.2.5. Physical Penetration Testing to evaluate the physical security controls in place, such as access controls, CCTV systems, and physical barriers,

to identify potential weaknesses that could lead to unauthorized physical access.

4.2.6. Cloud Infrastructure Penetration Testing to assess the security of cloud-based infrastructure, including platforms such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud, to identify configuration errors, access control issues, or vulnerabilities within the cloud environment.

4.2.7. IoT (Internet of Things) Penetration Testing on assessing the security of IoT devices, such as network-connected automation devices, fingerprint readers, access control devices, industrial control systems, and fire alarms to identify vulnerabilities that could be exploited by attackers.

4.3. Consultant shall consult with DNR at all times in the conduct of the VAPT Services. Findings and recommendations shall be kept classified and presented according to the severity, and immediately notify the DNR of any critical vulnerability even prior to the actual report issuance and report to the PMU that DNR has been notified as such.

4.4. Tests shall be conducted on the production environment and therefore, no destructive tests shall be executed. Penetration testing shall be confined to assessing whether the vulnerability could be exploited and in no circumstance shall the external perimeter be crossed. Therefore, clearly defined Rules of Engagement (ROE) for the VAPT must be prepared to ensure that the testing process is conducted ethically, legally, and securely. The following ROE are not exhaustive and may vary during the planning.

4.4.1. Scope Definition: Clearly define the scope of the VAPT, including the target systems, networks, applications, and specific testing objectives. Ensure all stakeholders (DNR, MoCCEE and PMU) agree on the scope before initiating any testing activities.

4.4.2. Authorization and Permission: Obtain written permission from the DNR of the systems and networks to be tested. Ensure that proper authorization is in place before starting any VAPT activities.

4.4.3. Non-Destructive Testing: VAPT should be performed in a non-destructive manner. Avoid actions that could cause system crashes, data loss, or any negative impact on the target environment.

4.4.4. No Data Manipulation: Under no circumstances should the VAPT consultant attempt to modify, transfer / relocate, or access sensitive

data, personal information, or any confidential information unrelated to the testing objectives.

4.4.5. Respect Privacy: The consultant must respect user privacy and not perform any actions that may violate the privacy of individuals or organizations.

4.4.6. No Exploitation Beyond Scope: Exploitation of vulnerabilities should be limited to the scope of the engagement. Any unintended discoveries should be reported and not exploited without proper authorization.

4.4.7. Confidentiality and Nondisclosure: All findings and sensitive information related to the VAPT should be treated as confidential and not shared with unauthorized individuals or third parties.

4.4.8. Legal Compliance: Ensure that all VAPT activities are conducted in compliance with applicable laws, regulations, and policies of the relevant jurisdiction(s).

4.4.9. Time Restrictions: Set a specific time window for the testing activities to prevent any negative impact on the target environment during critical business hours.

4.4.10. Communication with Stakeholders: Maintain open and clear communication with stakeholders, including periodic updates on progress, major findings, and any critical issues that may arise during the engagement.

4.4.11. Reporting Requirements: Agree on clear reporting guidelines for presenting the results of the VAPT with DNR, including a comprehensive summary of vulnerabilities, their severity, and recommended mitigation strategies.

4.4.12. Emergency Procedures: Define emergency contact and escalation procedures in case any critical issues or unexpected incidents occur during the testing.

4.1. Post-Engagement Cleanup: After the VAPT is completed, ensure that all testing tools and artifacts are removed from the target systems and that the environment is left in its original state.

4.2. The Consultant must have their own tools for tests that would be required to assess system vulnerability.

5. DELIVERABLES AND TIMELINE

Based on the above-described general scope of work for this assignment, in close coordination with D'MADD project's Project Management Unit (the PMU) and DNR, Consultant shall be responsible for delivering the below outputs:

Deliverable	Delivery
5.1. Approved Detailed VAPT Assessment Plan containing Test Plan, Methodologies, Objectives, Scope of Boundaries and Schedules	10 Business days from signing of contract
5.2. Execution of Vulnerability Assessment and Penetration Testing for the identified per the Scope of assignment	Within 20 Business days from Item 5.1
5.3. Report approved by the DNR of the VAPT assessment covering the following details. a) Executive Summary: A concise summary of the penetration test findings and recommendations, tailored for management and non-technical stakeholders. This summary should highlight the key vulnerabilities and their potential impact on the organization's security. b) Penetration Testing Report: A comprehensive report detailing the findings of the penetration test, including identified vulnerabilities, their severity levels, and recommended mitigation actions. The report should provide a clear overview of the security posture of the tested systems and applications. c) Risk Rating and Prioritization: A risk rating or scoring system for each identified vulnerability, helping the organization prioritize remediation efforts based on severity, likelihood of exploitation, and potential impact on the business. d) Technical Documentation: Detailed technical documentation, including step-by-step procedures, screenshots, and code snippets, that reproduce the identified vulnerabilities. This documentation should assist the organization's technical teams in understanding and resolving the vulnerabilities effectively. e) Proof-of-Concept (PoC) Exploits: PoC exploits that demonstrate how specific vulnerabilities can be	Within 15 Business days from Item 5.2

exploited, along with detailed instructions for reproducing the exploitation process. This helps organizations understand the real-world implications of vulnerabilities and validate their existence. f) Recommendations for Remediation: Specific and actionable recommendations for mitigating each identified vulnerability, including best practices, configuration changes, patches, or updates that need to be implemented to improve the security posture. g) Compliance and Regulatory Guidance: Guidance on how the organization can align with relevant compliance frameworks and regulatory requirements, ensuring that the security measures meet the necessary standards. h) Support: Optional post-assessment support, which may include clarification of findings, assistance with remediation efforts, and guidance on implementing long-term security measures. i) Training and Awareness: Recommendations for staff training and awareness programs to educate employees about common security risks, safe computing practices, and incident response procedures.	
5.4. Presentation of final findings (with revisions suggested by DNR) to the Senior Policy Makers	Within 5 Business days from Item 5.3

6. FEES

The Consultant is required to provide a comprehensive flat fee, including all costs and tax. This fee should be based on the deliverables specified in (Section 5) of the TOR. The fees should be quoted in Maldivian Rufiyaa (MVR).

It is important to note that the quoted lump-sum fee will remain unchanged, regardless of any potential increase in the consultancy duration, as long as the predetermined outputs are satisfactorily delivered.

7. PAYMENT SCHEDULE

Payment will be made in full to the consultant by the PMU, upon submission of the all the deliverables, conditional upon the DNR's approval.

8. INTELLECTUAL PROPERTY

All information pertaining to this project (documentary, audio, digital, cyber, project documents, etc.) belonging to the client, which the consultant may come into contact within the performance of his/her, duties under this consultancy shall remain the property of the client who shall have exclusive rights over their use. Except for purposes of this assignment, the information shall not be disclosed to the public nor used in whatever manner without written permission of the Client in line with the national and International Copyright Laws applicable. All the material used in the project should be provided to the client with copyrights cleared.

9. INSTITUTIONAL ARRANGEMENTS, REPORTING AND SUPERVISION

9.1. The consultant will work under the guidance and direction of the DNR and the D'MADD PMU will be coordinating the assignment.

9.2. Unless approved and agreed by the D'MADD PMU, the consultant shall not directly communicate, obtain, or share any documentation with any other party except DNR.

9.3. The consultant shall report to the Project Manager of the D'MADD Project PMU and DNR, on the status of the assignment on a regular basis. The consultant will work in a place agreed with the PMU and will be required to take part in all the relevant meetings.

9.4. All reports shall be submitted as stipulated in the deliverables and all reports will be submitted as drafts and upon review by the DNR, the Consultant shall revise the draft reports. Once the revised reports are accepted by the DNR they will be termed as final reports by the PMU to process the payments.

9.5. All draft documents should be in Microsoft Word and all final documents in Adobe Acrobat format with relevant signatures where needed.

9.6. All materials developed under this TOR shall be approved by the DNR.

9.7. The Consultant shall ensure that all outputs are delivered on time, and in accordance with quantity, quality and timeframe in the proposal submitted by the consultant based on the TOR.

10. QUALIFICATIONS AND EXPERIENCE

10.1. Bachelor's degree in cyber security/ computer science/ computer security/ network security or in a related field, with a minimum of 5 years of experience in cyber security/ computer science/ computer security/ network security or in a related field.

OR

Professional Certification: The consultant conducting the penetration testing and audit should have a valid certification from a trustworthy and industry well-known cyber security assessment certification body. This certification should demonstrate their expertise and knowledge in cybersecurity, including the latest industry

standards and best practices, with a minimum of 5 years of work experience in the field of cyber security/ computer science/ computer security/ network security or in a related field in an organization.

10.2. Prior IT Security Penetration Testing and Audit Experience: The consultant should have prior experience in conducting IT security audits, with continuous work in the field for the past 5 years. This experience should demonstrate their ability to identify and address cybersecurity risks and vulnerabilities in complex and large-scale organizations.

11. REQUIRED DOCUMENTS

11.1. Reference letters and certifications as proof of the qualifications and experience in Section 10. The reference letters may include work experience letters as well as contract services successfully provided as a freelance individual consultant.

12. EVALUATION CRITERIA

12.1. Selected candidate/Consultant must meet all requirements identified under Section 10.

12.2. A contract will be awarded to the substantially responsive candidate with highest technical score above the 70% pass marks and after successful negotiation of contract price.

The Consultant will be selected based on the following criteria:

Criteria	Points
Educational Qualifications (10.1)	30
Specific work experience in the field of cyber security/ computer science/ computer security/ network security or related field *(5 points will be awarded for each year of experience)*	40
Prior IT Security Penetration Testing and Audit Experience (10.2) No. of penetration testing assignments and IT security audits *(5 points will be awarded for each completed assignment)*	30

13. SUBMISSION

13.1. The deadline for submission of the Expression of Interest is before *10:00am* on *April 25th, 2024.*

13.2. You may submit your Expression of Interest through postal mail or by hand-delivering them in sealed envelopes addressed to the Project office.

Project Manager
Digital Maldives for Adaptation, Decentralization and Diversification Project (D'MADD)
Ministry of Climate Change, Environment and Energy
NCIT Building
No 64, Kalaafaanu Hingun, Male' 20064, Republic of Maldives
Tel: +(960)330-2253
Email: procurement.dmadd@environment.gov.mv

ANNEX 1

Comprehensive list of coverage area for Vulnerability Assessment and Penetration Testing (VAPT)

To identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system through a variety of automated tools combined with manual verification of identified issues. VAPT should be comprehensive, including but not limited to the following listed activities. The consultant should provide, advice regarding VAPT and the necessary activities as part of their proposal.

1. Attempting to guess passwords using password-cracking tools.
2. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
3. DDOS and brute force attacks, phishing attacks (to expand)
4. API data breaches, auditing and logging mechanism assessment
5. Check if any Vulnerability exists in the Servers, Database, Applications, Network and Security devices in scope without disturbing operations.
6. Sniffing Data or information.
7. To check whether there is any vulnerability present in all IT assets in scope.
8. To ascertain the configuration, placement and deployment of IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized.
9. Vulnerabilities of unnecessary utilities residing on Application server.
10. Unnecessary ports or services open/ running on the servers.
11. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
12. If any cases of unauthorized access through hacking, denial of service due to technological failure is possible.
13. Any other items relevant in the case of security, to be included in commercial bid and not to be considered an addition cost.

14. The assessment should include following sections for testing as agreed with Client: -
    a. Testing done through an external network
    b. DMZ Zone
    c. Remote Access
    d. Network Security Assessment
    e. Network Security Components
    f. VPNs
    g. VC & VoIP Communications Network.

15. Provide scheduled updates regarding the project.

16. Provide documents / diagrams detailing the project information in a timely manner.

17. Network Scanning /Surveying: Consultant shall identify active hosts on a network, for the purpose of simulating attack and also for network security assessment with the help of suitable procedure/tools including but not limited to: -
    a. Examine Name server responses.
    b. Review the outer wall of the network.
    c. Review tracks from the target organization.
    d. Review Information Leaks

18. Port Scanning: To find the active ports on server port addresses on a host Consultant shall perform the following but not limited to:-
    a. Error Checking
    b. Enumerate Systems
    c. Enumerating Ports
    d. Verification of Various Protocol Response
    e. Verification of Packet Level Response

19. Port sweep: To scan multiple hosts for a specific listening port for potential vulnerabilities.

20. System & OS Fingerprinting: To guess the system information i.e, type and version of OS etc.

21. System Identification & Trusted System Scanning: Consultant shall perform the SITS scanning which would include but not limited to the following :-
    a. Match each open port to a service and protocol.
    b. Identify server uptime to latest patch releases.
    c. Identify the application behind the service and the patch level using banners or finger- printing.
    d. Verify the application to the system and the version.
    e. Locate and identify service remapping or system redirects.
    f. Identify the components of the listening service.
    g. Use UDP-based service and Trojan requests to all the systems in the network.

22. Wireless Leak Tests: Consultant shall perform the vulnerability assessment & wireless leak test. This may include the following activities: -
    a. Verification of the distance in which the wireless communication extends beyond the physical boundaries of the organization.
    b. List equipment needed/tried should be taken (antenna, card, amplifier, etc.)
    c. Verification of authentication-method of the clients.
    d. Verification of that encryption is configured and running - and what key length used.
    e. Verification of that clients can't be forced to fall-back to plaintext-mode.
    f. Verification of the IP-range of the network
    g. Verification of the IP-range and reachable from the wireless network, and the protocols involved.
    h. Probe network for possible DoS problems.

23. Vulnerability Scanning: Consultant shall carry out VA for entire IT assets provided by the DNR upon successfully contracting of the Consultant.

24. Malware Scanning: Consultant shall do exhaustive scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

25. Spoofing: Consultant shall assess the scope of potential spoofing attacks i.e., IP, ARP etc. and other applicable ones in the organization environment

26. Security Policy Review: Consultant shall carry out the review & assessment of Security Policies already in place in firewalls installed in the organization.

27. Services Probing: Consultant shall do the following in connection with the following:
    a. Web Tracks
    b. Mail Tracks
    c. Name Services
    d. Visible Documents
    e. Anti-Virus and Trojan

28. Application Security Testing & Code Review: In case of some application whose code review is allowed to be done for the purpose of VAPT i.e, RMS, CLMAS, ECM, OSS, ENSURE, NABNET, ILMS etc. the Consultant shall conduct the same.

29. Service Fingerprinting: The Consultant shall do the following: -
    a. Examine system responses to determine operating system type and patch level.
    b. Examine application responses to determine operating system type and patch level.
    c. Verify the TCP sequence number prediction for each live host on the network.
    d. Search job postings for server and application information from the target.
    e. Search tech bulletin boards and newsgroups for server and application information from the target.
    f. Match information gathered to system responses for more accurate results.

30. Access Control Mapping: ACL has to be reviewed and recommended for improvement.

31. Assessment of OS Hardening: Consultant shall carry out the assessment of OS hardening to check & explore the gap in hardening, patch management etc.

32. Denial of Service (DOS) Attacks: Following points may be looked for DoS attack.
    a. Verify that administrative accounts and system files and resources are secured properly, and all access is granted with "Least Privilege".
    b. Check the exposure restrictions of systems to non-trusted networks.
    c. Verify that baselines are established for normal system activity.
    d. Verify what procedures are in place to respond to irregular activity.
    e. Verify the response to SIMULATED negative information (propaganda) attacks.
    f. Test heavy server and network loads.

33. DDOS Attacks: All the steps as mentioned for DoS attack has to be verified.

34. Authorization Testing: Consultant shall do the authorization & authentication testing for the present AD or AZAD.

35. Doc Grinding (Electronic Dumpster Diving)

36. Lockout Testing: To mitigate the brute force attack etc., lockout testing must be carried out.

37. Password Cracking: To mitigate the brute force attack, cryptographic attack etc., Password cracking testing must be carried out.

38. Cookie Security: Consultant shall review the cookie settings and recommend the best practice for making the environment secure.

39. Cookie & Web Bug Analysis: Consultant shall review the cookie for bugs and recommend the best practice for making the environment secure.

40. Functional validations: Any or all application when offered for functional validation, Consultant shall perform the same.

41. Containment Measure Testing: The Consultant shall perform this test also wherever applicable.

42. War Dialling: In case of need Consultant would carry out the war dialling for fax machines.

43. DMZ Network Architecture Review: Consultant shall review the present DMZ Network Architecture and recommend for the improvement if any.

44. Server Assessment (OS Security Configuration): Consultant shall review the present configuration of critical servers and recommend for the improvement if any.

45. Security Device Assessment: Consultant shall review the present security devices and recommend for the improvement if any.

46. Network Device Assessment: Consultant shall review the present network devices and recommend for the improvement if any.

47. Database Assessment: Consultant shall review the present databases and recommend for the improvement if any.

48. Website Assessment (Process): Consultant would do the assessment of internet facing application as mentioned in the subsequent section with and without credentials having different access levels like operator, supervisor, administrator, etc, to check for vulnerabilities like privilege escalation, input validation, etc.

49. Vulnerability Research & Verification: Consultant shall conduct the research including but not limited to the following: -

a) Integrate the currently popular scanners, latest scanning definitions/signatures, hacking tools, and exploits into the tests.

b) Measure the target organization against the currently popular scanning tools.

c) Attempt to determine vulnerability by system and application type.

d) Attempt to match vulnerabilities to services.

e) Attempt to determine application type and service by vulnerability.

f) Perform redundant testing with at least 2 automated vulnerability scanners.

g) Identify all vulnerabilities according to applications.

h) Identify all vulnerabilities according to operating systems.

i) Identify all vulnerabilities from similar or like systems that may also affect the target systems.

j) Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.

k) Verify all positives. In addition to the above Consultant shall perform Manual Vulnerability Testing and Verification also.

l) IDS/IPS review & Fine tuning of Signatures: Consultant shall perform the IDS /IPS review including but not limited to the following:-
    a. IDS and features identification
    b. Placement of IDS in the network
    c. Testing IDS configuration
    d. Reviewing IDS logs and alerts

m) Man in the Middle attack: - To rule out the possibilities of eavesdropping the MIMA has to be accrued out.

n) Man in the browser attack: To rule out the possibilities of eavesdropping the MIBA has to be accrued out.

o) Social Engineering: The Consultant shall carry out social engineering for Employees at DNR or Other points of NRIVS related Institutes staff & Administration.

This may include request testing, guided testing & trusted people testing. This may include the following but not limited to:-

i) Select a person or persons from information already gained about personnel
ii) Examine the contact methods for the people from the target organization
iii) Invite the people & Gather information from them
iv) Enumerate the type and amount of privileged information disclosed.

p) Trusted Systems Testing: The validity of trusted system also has to be checked. Directory Traversal: Directory Traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.

q) Linux Hacking: Consultant would assess the security risk associated with systems running on Linux platform.

r) Key loggers: Key loggers are a form of spyware where computer users are unaware their actions are being tracked.

s) Rootkit: Consultant would assess the systems to see the presence or probability of presence of rootkit.

t) Botnet: Consultant would assess the system to see the presence of botnet.

u) Any other attacks & Scenario Analysis: Apart from all the above-mentioned line item if any activity required.