Supercomputer Education and Research Centre

Indian institute of Science,

Bangalore

RFP No. SERC/NBK/DoT-Tools/10/2018

Proposals are invited, in two-cover format, from bidders for the following Security Testing Tools/ equipment's

1. Network and Application Protocol Fuzzers
2. Source Code Analyser (Static)
3. Vulnerability Scanners (TCP/IP based applications) with full plug-ins
4. Penetration testing Tool
5. OS Hardening Tool
6. NTPC Server
7. Spectrum Analyser

Detailed technical specification for each of the above is given as annexures A-G

1.0. Bidder Eligibility Criteria

a) Bidder should be either OEM or his authorised agent. If bidder is an authorised agent then he should submit documentary proof that he has been authorised to submit bid for this enquiry.

b) The bidder should have a track record of having previously supplied similar equipment.

c) The bidder must have a proven record of maintaining and managing the similar system in India. Purchase order copies of previous installations are required along with customer contact details

d) The bidder should have qualified technical service personnel based in India for supporting the tool/equipment.

e) The bidder should be in a position to demonstrate their competence and capability, as a team, to deliver all the services expected during the contract period.

f) In case the bidder is an authorised representative for the OEM the technical bid should clearly demarcate the responsibilities between the OEM and the bidder. Complete details of the same have to be submitted along with the bid.

2.0 Submission of Proposal

a) The quotation should be in Two-cover format – a Technical part and Commercial part for each enquire within this RFP

b) Covers containing the technical and commercial bids must be individually sealed and superscribed respectively as "Technical Bid" and Commercial Bid" along with Enquiry ref no. as given in the annexures.

c) The two covers must be put in a larger enveloped, sealed, superscribed with Enquiry ref no. as given in the annexures.

d) All the covers should bear the name and address of the bidder.

e) Bidder can quote for one or more of the items indicated in this RFP

f) Non-conformance of any of the above can result in disqualification. All the pages must be signed by the bidder.

2.1 Technical Bid

The technical bid should contain the following.

- Detailed Technical description of the product proposed.
- Compliance statement indicating its meets the each and every clause in the terms and conditions, technical/commercial specification
- Unpriced bill of material with quantities of each line item.
- Datasheet of product/model
- Undertaking to support the tool/equipment is given in Form A, it must be signed by the OEM enclosed as part of the Technical Bid.
- If the bidder is not the OEM, then appropriate letter from the OEM should be submitted authorizing the bidder to submit proposal for this RFP
- Bids has to quote exactly as per mentioned specifications for entire solution, partial offers will not be accepted.

The technical bid should not contain any price information. Non-conformance will result in disqualification.

2.2 Commercial Bid

a) The Commercial bid should contain details of the prices for each one of the subsystems of the total offer giving clearly the rate and the quantity. Bundling of the prices is not acceptable.

b) Bidders proposing multiple options must quote for each of the configurations separately.

c) Warranty charges, if any, must be quoted separately.

d) In addition AMC charges for additional Year 2 and Year 3, should be quoted separately.

3.0 Installation, Warranty, Annual Maintenance, Training and Support

a) The total solution as per the bill of materials has to be supplied within 4 weeks after receiving a firm PO from IISc

b) The installation and commissioning of the tool/equipment should be completed within a week after supply of the equipment.

c) Alternatively Installation and commissioning of the tool/equipment should be done with 5 week of release of Purchase Order.

d) Warranty services

1. Should be for a period of one years from the date of acceptance of the equipment.
2. The bidder shall be fully responsible for the warranty in respect of proper design, quality and workmanship of all the systems supplied.
3. The bidder shall attend to all the hardware problems on site and shall replace the defective parts at no extra cost to the purchaser.
4. the preventive maintenance and repairs of the components supplied by the bidder are the responsibilities of the bidder
5. Software updates must be promptly done.

e) Annual Maintenance

1. Annual Maintenance Contract services should be valid for a period of two years after warranty period..
2. The Bidder or OEM shall provide patches/updates for any software bug, noticed from the date of supply till the end of contract at no extra cost to the purchaser.
3. Upgradation of the tools shall be intimated by the supplier within one week from the date of release.
4. Any hardware, software, firmware which is required as a pre-requisite to support upgradation shall be provided free of cost. Any specific training to utilize the upgraded feature shall be provided on site by the supplier at no extra cost to the purchaser

f) Detailed Hands –on Training shall be provided for 10 officials on Configuration/usage of tool equipment's supplied

g) These tools/equipment are purchased as part of a project from Dept. of Telecommunication (DoT), Govt. of India. The tools/equipment along with the licences will be transferred to a DoT, Govt of India or any other organization under its administrative control. The bidder must give an undertaking to continue to support the same. (Form A)

h) The OEM must give an undertaking to provide service for 10 years, in case OEM is taken over by the new entity must continue to provide the service without any break.

4.0 Additional Guidelines:

a) IISc is eligible for customs exemption under notification 10/97-ce. Bidders planning to quote any imported solution have to give the offer in the US dollar.

b) The offer has to clearly explicitly state the supply part, Warranty services and any other charges separately.

c) Delayed and/or incomplete tenders are liable to be rejected.

d) All the pages of Technical Bid and the Commercial Bid should be duly signed by the bidder.

e) Commercial bids of technically qualified bids alone will be taken up for further processing.

f) The Director, IISc, Bangalore-12 reserves the right to modify the technical specifications or the required quantity at any time.

g) The Director, IISc reserves the right to accept or reject any proposal, in full or in part, without assigning any reason.

h) The bidders are requested to go through the Terms and Conditions detailed in this document, before filling out the tender. Agreeing to the terms and conditions of the tender document (by signing all pages of the copy of a tender document) is a mandatory requirement

i) A tender, not complying with any of the above conditions is liable to be rejection.

j) The Bid must be set the following Address,

Project "National Telecom Testbed"
Room NO. 406
Supercomputer Education and Research Centre
Indian Institute of Science
Bangalore 560 012

5.0 Commercial Terms and Conditions

a) The commercial bid should contain among other things, payment terms, warranty, installation and commissioning charges. These charges will be paid only after successful supply, installation and acceptance.

b) Prices may be quoted in US Dollars. (if applicable).

c) Vendor should quote the prices for shipment on 'CIF' terms.

d) Withholding tax, if applicable, will be deducted from the bid amount.

e) In case of imports, the commercial bid should contain among other things the name and address of the Indian agent, if any and the agency commission payable to him. Agency commission part will be deducted and will be paid to him separately in equivalent Indian rupees.

f) In respect of imported solution, IISc will arrange for customs clearance, at Bangalore airport, which will be final destination airport. Hence costs related to customs/clearance need not be included in the offer.

g) In CIF offers of imported solutions, insurance should be on “Warehouse to Warehouse” basis and should not terminate at Bangalore airport.

h) In case of rupee offer, the tax component should be shown separately and not included in the total amount, to enable us to avail exemption.

i) Price should be quoted per unit and the total amount for the required quantity.

j) Offer should be valid for 60 days from the date of submission

6.0 Payment Terms

The conditions regarding payment terms are as follows:

1. The total project cost will consists of two parts:
    a. Equipment supply part (Supply)
    b. Installation, commissioning, warranty and maintenance services part (shortly referred as services), if applicable.
2. The total cost of the system (Supply part) will be paid through SIGHT DRAFT/Letter of Credit (documents through Bank)
3. Installation charges, if any, payable only in Indian Rupees, will be paid after acceptance of the system. The procedure is as follows: On delivery complete inventory checks mandates confirmation of systems to have been delivered with the ordered configuration. Post installation burn-in test for 48 hours will be performed. The burn-in test includes running of hardware diagnostics on all components continuously for a period of 48 hours to eliminate possibility of any hardware failures. The successful completion of the acceptance test will results in payment.

Contact Person:
For any queries or clarification the following person may be contact through email (Project48office.serc@iisc.ac.in) with subject as “Telecom Test Bed Project Purchase”

SERC, IISc, Bangalore.

Important Dates:

IISc Web publication	20 July 2018
Last day for queries, if any, only by email	27 July 2018
Pre-bid clarification Meeting	03 August 2018
Last date for submission of bid on or before	17 August 2018

Form A

Undertaking to Support the Equipment/software

The Bidder along with the OEM note that the equipment/software tendered are being purchased for a project funded by Dept. of Telecommunication (DoT), Govt. of India(GoI) to Indian Institute of Science(IISc). These software/equipment to be transferred to DoT or any other unit/organization under DoT. When these equipment/software are transferred, we agree to continue to support/service/upgrade the same under the same terms and conditions under which they are purchased.

The licences will be transferred as and when it is request from Indian Institute of Science without any additional cost.

From the time the equipment/software are transferred all financial commitments will be with organization to which the equipment/software is transferred.

Original Equipment Manufacture

Signature with Date
Name:
Designation:

:

Annexure A

Network and Application Protocol Fuzzers

a. Enquiry No. SERC/NBK/NAPF/2018

b. Quantity: One

b. Technical Specifications

Functional & General:

i. Any additional existing standard/proprietary telecom protocol as requested by TTSC to be supported in future within a short notice of 2 months.

ii. Client-server based arrangement for all the protocols mentioned in Table 1.

iii. Tool shall be upgraded by the supplier, for new protocols, with generation based fuzzing for telecom protocols defined in the relevant standards e.g. ITU-T, 3GPP, IETF etc within a time frame of 2 months from the date of release of standard documents.

iv. The tool should be installable & executable on all popular OS (Operating System) platforms with 32 bit and 64 bit versions (on Personal Computers).

v. Along with automated fuzzing, tool shall also enable the tester to manually set the fuzzing parameters such as test runs, logging behavior, fault identifying, network interface options, test time & instrumentation etc depending on his own criteria and carry out fuzzing. Any technical support in this regard should be provided by the supplier.

vi. Tool shall enable the tester to pause/stop fuzzing whenever required.

vii. The tool should be capable of checking interoperability between Test tool and DUT for all the protocols mentioned in Anex I.

viii. All software licenses of protocol fuzzing test suites should be dongle based and of perpetual (life time) validity.

Testing & Reporting capabilities

i. Tool shall be capable of fuzzing the protocols listed in Table 1 as per relevant standards such as 3GPP, IETF, etc that define these protocols. (Tentative List of protocols that should be supported are attached in Table 1)

ii. The tools shall support Generation(RFC) based fuzzing for all the protocols given in Annexure I. It shall be capable of generating different types of malformed protocol messages to simulate attacks for testing the robustness of protocols supported by the DUT.

iii. The tool shall be dynamic and stateful with in-built complete protocol state machines and shall support fuzzing by adding anomalies in the protocols at the level of message sequencing, message types, message structure ordering, message field value and other message aspects that a protocol supports in a real operating environment

iv. The tool shall support automatic generation and execution of fuzz test cases or pre-built test cases for all the protocols listed in Annexure I and there shall be no development required from the Tester for automated fuzzing

v. The tool shall provide necessary built-in and extendable health check mechanisms for monitoring the impact of the fuzz test cases on the Device Under Test (DUT). The tool shall support both in-band and out-of-band instrumentation. In-band instrumentation is used to obtain the crash - no crash status and usually consists of sending a valid protocol request to the DUT. The tool shall support both SNMP checks and Syslog checks as out-of-band instrumentation methods used to obtain DUT state information.

vi. The Tool shall be able to identify success and failure in terms of whether the DUT was able to withstand the attack or not.

vii. Tool shall be capable of identifying the following responses of the DUT to the fuzz testing:

- The DUT crashes and is unable to restart
- The DUT crashes and then possibly restarts.
- The DUT hangs in a busy loop, causing a permanent Denial of Service situation.
- The DUT slows down momentarily causing a temporary Denial-of- Service situation.
- The DUT fails to provide useful services causing a Denial-of-Service situation (i.e. new network connections are refused)

viii. It shall be possible for the tester to choose the test cases to be run as per need, based on protocol PDU fields, message type, etc. It shall also be possible for the tester to run the most effective attack patterns for different fields of the protocol to keep the test run time reasonable.

ix. The tool should be capable of checking interoperability between Test tool and DUT for all the protocols mentioned in Annexure I.

x. The Tool shall provide user friendly GUI as well as command line interface for operation and handling of Fuzzing tool. It shall also support easy configuration of test related parameters.

xi. The tool shall provide accurate and unambiguous analysis of every test case run using the tool and identify potential reasons for failure including CVSS scoring of identified issues and CWE classification of test cases.

xii. The tool shall allow the tester to reproduce the failed test cases and confirm the results.

xiii. Once the fuzz testing is started, the tester shall know, at all times, the current stage of fuzz testing with appropriate status messages.

xiv. The tools shall maintain a detailed log of the fuzz testing and it shall be possible for the tester to access the log details at any time. It shall be possible to export the log file to an external storage in standard file formats that will enable viewing of the test information at any point of time.

xv. The Tool shall support generation of comprehensive reports for the tests carried out. For every test case it shall be possible to obtain detailed information with regard to the status of DUT before test, the input fuzz message sent, DUT’s response to the fuzz message and in case the test case fails the potential reasons for the abnormal behaviour of the DUT.

xvi. The tool shall be able to correlate the cause and effect between the specific test case(s) and the abnormal behaviour. For every fault identified, it shall provide data containing test logs, packet captures and all the test run information necessary for accurate reproduction of the behaviour.

xvii. Report should also figure in the statistics for a given testing task across types of attacks, types of failures and interfaces including total number of failed cases and DoS time caused by test case/group of test cases, if any.

xviii. Report shall also provide prioritization of the detected vulnerabilities highlighting the most critical problems first.

xix. The tool supplier shall provide a suitable on-site mechanism to customize the contents (i.e data needs to be included in the report) ~~format~~ of the report generated by the tool as per the requirement of the Tester. Standard test report formats such as PDF/HTML/XML shall be supported.

xx. In the event of power failure during testing or when the fuzzer abruptly shuts down due to other reasons, the fuzzer tool shall resume the testing from the point at which the shutdown occurred. It should not happen that the tool starts performing the fuzzing from the beginning.

xxi. Well documented user manual should be made available for the intended purpose.

Table 1

S.No	Protocol	S No	Protocol
1	BGP4	18	PTP
2	DHCPv4	19	RADIUS
3	DHCPv6	20	RIP
4	Diameter (includes S6a,S13, Cx, Gx, Rx, Sh, S3)	21	RIPng
5	GTPv1	22	RLC
6	GTPv2	23	RRC
7	HTTP/HTTP 2	24	S1AP
8	HTTPS	25	SCTP
9	IKEv1/v2/ISAKMP	26	SNMP v3/SNMP trap
10	IPSec (AH, ESP, RFC 4305)	27	SSHv2
11	IPv4 Suite(includes ICMP. ARP,IGMP)	28	Syslog
12	IPv6 Suite (includes ICMP)	29	TACACS+
13	LDP	30	TCPv4
14	MPLS	31	TCPv6
15	NTP	32	TLS v1.2
16	OSPFv2 / v3	33	UDPv4
17	PDCP	34	UDPv6
		35	X2 AP

Annexure B

Testing Tool Name: Source Code Analyzer (Static)

a. Enquiry No. SERC/NBK/SA/2018

b. Quantity: One

c. Technical Specifications

The Tool shall be able to operate 100% on premise and offered as a software product and Scan results should always be available on premise. Barring the features that are specifically stated as optional, this tool shall mandatorily meet all the technical specifications stated below.

i) Ease of use of the tool

a) No Setup and runtime dependencies shall exist i.e. tool should run only on build of the source code without asking the user for any additional inputs that are known to only developer of the source code such as names of the library functions/header files, values for macros/command line variables, search path and so on.

ii) Deployment Model

a) On premises Installation on local machines/tool Server

b) No cloud based solution

c) Client –server model or node lock using dongle

d) Supply of online/offline Installation manual and Operation Manual

e) Support for all prevalent platforms such as Linux, UNIX, Windows and so on

iii) Support for high level Programming languages

a) Ability to scan the code written in all the prevalent high level programming languages such as C , C++, Java and so on

b) Ability to extend its scope to include non-standard source code file extensions such as JSPF

iv) Support for Secure coding Standards/Vulnerability Databases

a) Compliance to a minimum of two popular secure coding standards from the following list of secure coding standards prevalent today :

1. Cert C,
2. Cert Java,

3. Cert C++,

b) Ability to check the source code compliance against all the following prevalent secure coding vulnerability databases

1. CWE(Common Weakness Enumeration)
2. SANS TOP 25
3. OWASP TOP 10 – YEAR 2017

v) Software Updates/Upgrades to the tool

a) Updates and Upgrades with new versions of the existing/new coding languages/ scripts/ secure coding standards / vulnerability databases to be supplied during the entire period of contract within 30 days from the date of the release of the new versions.

b) Support for backward compatibility of the Updates/upgrades i.e scripts from previous version can be reused with later versions.

c) Updates/upgrades shall be provided promptly as software patches , preferably in CD form such that they can be loaded to the tool locally inside the organization's premises without the need to connect to the internet or any other external network.

vi) Technical support, Training and License

a) Local support at Bangalore

b) support on need basis

c) Suitable on-site mechanism to report the technical problems/issues

d) One week Training on premises of the buyer organization

e) Software with perpetual License with life time validity

vii)Scan, command and control support

a) Command Line (CLI) Support

b) User friendly GUI , preferably Web based GUI Support

c) IDE support (optional)

viii) Scan Configuration and Customization capabilities

a) Ability to package the scan rules selectively and to run selective sets of rules.

b) Support for User defined Coding standards & rules compliance check

c) Selective Scanning ability

d) Incremental Scanning ability

e) Scheduled Scanning ability to schedule the scan upto 24 hours in advance

f) Saving and re using the scan configuration feature

g) Ability to run simultaneous multiple scannings

h) Support for Concurrent multiple users

ix)Scanning and Remediation capabilities

a) Ability to conduct various kinds of analysis on the source code such as dataflow analysis , control flow analysis, information flow analysis , pattern-based (rules-based) static analysis and so on

b) Automatic Scanning to identify all the Known vulnerabilities and their exact location in the code

c) Ability to correlate and prioritize the scan results according to the severity such that the most serious issues are displayed first.

d) Ability to provide details such as description of the vulnerability , its severity , location , data flow , control flow and so on are provided by the tool

e) Ability to provide the Remediation advice for each finding of vulnerability on how to fix it at the line-of-code level along with examples in the same programming language to be provided by the tool

x) Report Generation and Presentation capabilities

Following reports shall be generated by the tool in PDF and XML format and optionally, in text/ html format:

a) Technical Detailed Report providing the detailed technical information about the vulnerability such as Summary of the issue including the weakness category , Location of the issue including file name and line of code number, Remediation advice along with code samples in the same programming language, Data Flow Details which indicates the tainted data flow from the source to the sink ,Control flow details and so on.

b) Compliance Reports which quickly determine whether the code is in violation of the secure coding standards/vulnerability databases.

c) Summary reports such as Issue category wise reports (memory leaks, API abuse, buffer overflow and so on), Severity wise reports , Configuration reports

d) Executive Summary report that provides high-level summary/overview of the scan results(optional)

xi) Graphical Reports generation capabilities (Optional)

a) Generation of the Control flow graphs and data flow graphs (optional)

b) graphical representation of all the summary reports (optional)

Annexure C

Vulnerability Scanners (TCP/IP based applications) with full plug-ins

a. Enquiry No. SERC/NBK/VS/2018

b. Quantity required: 3 Nos

c. Technical Specifications

The Tool shall be able to operate 100% on-premise and offered as a software product and Scan results should always be available on premise.

I. Vulnerability assessment tool supplied shall be capable of scanning targets i.e. network nodes including end user devices, the operating systems, databases, and/or Web applications residing on those nodes in an attempt to detect known vulnerabilities

II. The tool shall be able to support installation on Linux and Windows (10 and later versions) Operating Systems

III. The identified vulnerabilities shall comply to latest NVD/CVE catalogue

IV. The tool shall be capable of doing scan targets which can be in a variety of formats i.e. IPv4/IPv6 addresses, hostname, and CIDR notation.

V. The supplied tool shall begin its assessment by performing a “footprint” analysis that involves first discovering live hosts and all open ports on a host then scanning these ports to enumerate all of the available services on the device to determine which services and/or software programs (including versions and patch levels) are running on the target.

VI. The tool shall have the capability to perform both internal and external IP addresses scanning.

VII. The tool scans shall be user controllable, i.e. able to be started, stopped, paused and resumed at any time per user requirements.

VIII. The tool shall be able to schedule scans at specific starting dates and time, frequencies and maximum scan durations.

IX. The tool shall be able to automatically pause scheduled scans if unable to complete within the predefined durations.

X. Each purchased single user license of the tool shall support testing of at least 10 devices /IP's simultaneously

XI. The tool shall be upgrade the IP license to a larger in case need to scan more IPs

XII. The tool shall allow to change IP's

XIII. The tool shall have provision to support schedule scans run daily , weekly, monthly , yearly basis and on demand basis scans The tool shall support to configure e-mail addresses to receive scan notifications

XIV. The tool shall support Permissions functionality affects which users have permissions to access or configure the scan

XV. The tool shall be able to support both credentialed and non-credentialed scans which include but is not limited to: SNMP, SSH, WINDOWS

XVI. The tool shall run on Windows,Linux (all distributions) OS operating environment

XVII. The tool must support the automatic discovery of virtual assets on VMware

XVIII. The tool must support integration with IDS/IPS products.

XIX. The reports generated by the supplied vulnerability assessment tool shall also provide prioritization of risk (like critical, High, Medium, low and information) with CVSS (v2 and v3) score, exact remediation for individual vulnerabilities, and recommendations on how to fix and improve the security of the DUT,providing Information on availability of exploits and its reference links information of the discovered vulnerabilities

XX. The tool shall be with Default(in built) scan templates and allow user to configure customised scan template

XXI. The tool shall be able to integrate native exploit information from well-known sources, minimally with ExploitDB and Metasploit database.

XXII. The tool shall support integration with external penetration testing platforms to perform and automatic vulnerabilities exploitation

XXIII. The tool shall be able to identify known exploits and malware kits associated with detected vulnerabilities.

XXIV. The tool shall be able to generate / export reports in various formats such as but not limited to PDF, HTML, Text and XML.

XXV. The tool must include pre-configured report templates and must support report template customization from default available ones.

XXVI. The tool shall be capable to scan any type of OS (Operating Systems) and fingerprint their version information

XXVII. The library of the vulnerability assessment tools shall be updated on a regular basis with the most recent security vulnerabilities.

XXVIII. The supplier shall provide suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

XXIX. The supplier shall ensure the upgradation of library of known vulnerabilities on a daily basis in complete synchronization with the vulnerabilities published in the NVD/CVE catalogue

XXX. The tool vendor must develop their own vulnerability checks. Describe internal vulnerability development. Include any internal 0-day exploit development

XXXI. The tool shall be coded with maximum coverage of plugin's (which is a simple program that checks for a given flaw) covering of local and remote flaws

XXXII. The tool shall be able to perform both automatic & manual (Plugins/ Software updates)

XXXIII. The tool shall identify misconfigurations in target device like missing patches in OS/applications etc.

XXXIV. The tool shall support integration with Active Directory, Kerberos, or any LDAP compliant directory.

XXXV. The tool shall be able to perform discovery, vulnerability scanning, web scanning, and compliance assessment in a single scan.

XXXVI. The tool shall be with web application scanning solution must support coverage of OWASP TOP -10-2017

XXXVII. The tool shall capable of scanning the web applications to identify the programming errors such as cross-site scripting, remote file inclusion, command execution, traversal attacks, and SQL injection with the necessary plugin's

XXXVIII. The tool web-based mangament user interface shall be using the minimum version specified of the browsers are Internet Explorer 9 , Firefox ,Chrome

XXXIX. Software with perpetual License with life time validity

Annexure D

Penetration testing Tool

a. Enquiry No. SERC/NBK/PT/2018

b. Quantity required: 4 Nos

c. Technical Specifications

I. The Tool shall be capable of exploiting the vulnerabilities found on network elements,operating systems, desktop applications, Web applications, servers , databases and end user devices

II. The tool shall be able to support installation on Linux and Windows 10 and later versions) Operating Systems

III. The tool shall include web-based GUI and Command Line Interface

IV. The tool shall be able to run jobs or tasks (e.g. scan, exploit) on schedule

V. The tool shall have latest updates (e.g. exploit module) as frequent as on a weekly basis.

VI. The tool shall support manual software updates

VII. The tool shall conduct scans and discover the host's, Ports , OS and running services

VIII. The tool shall support importing of scan result from external tools including but not limited to Nexpose, NetSparker, Nessus, Burpsuite, Acunetix, AppScan etc

IX. The tool shall support brute force testing on services including but not limited to DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, Telnet, FTP, POP3, SNMP

X. The tool shall provide password references for factory default logins for brute force testing

XI. The tool shall support customized credentials and dictionary import for brute force testing

XII. The tool shall be able to apply exploits on individual IP or multiple IPs of a minimum of 10 Nos

XIII. The tool shall also have the capability of development of new customized exploits,as well as augmentation or modifications in the existing exploits.These customizations or modifications shall be possible with minimum efforts in any programming languages/scripts

XIV. The tool exploits shall be thoroughly tested prior to supply of the tool and a declaration to this extent be submitted by the supplier/developer

XV. The tool shall support running individual exploit module manually from the user interface

XVI. The tool shall support replay of exploitation tasks

XVII. The tool shall support web crawling on IPv4 and IPv6 web sites.

XVIII. The tool shall support detection of vulnerable URLs as per OWASP2013 TOP10 standards and later

XIX. The tool shall support web crawling a minimum of 4 Websites concurrently

XX. The tool shall provide built-in standard reports and support customized report functionality

XXI. The tool shall support report formats including but not limited to PDF, Word and HTML

XXII. The tool shall support reports to be stored locally and sent to recipient by email after created

XXIII. The tool shall be able to support export the generated reports

XXIV. The tool shall have latest software updates (e.g. exploit module) as frequent as on a weekly basis.

XXV. The tool shall support offline activation and manual updates

XXVI. The tool shall be able to run jobs or tasks (e.g. scan, exploit) on schedule.

XXVII. Software with perpetual License with life time validity

Annexure E
OS Hardening tool

a. Enquiry No. SERC/NBK/OSH/2018

b. Quantity required: 4 Nos

c. Technical Specifications

- **The Tool should be capable of testing and gathering (security) information from Unix based systems**
- **The tool should support self-hosted version which can runs within your IT environment.**
- Tool should be capable of giving priority based improvement plan for hardening of operating system.
- Tool should provide a means to check for a defined policy and report about the compliance with the policy.
- Tool should have capability to check compliance against regulations or standards such as PCI DSS, HIPAA, Sox etc.,
- Tool should support a web interface for management
- Tool should be capable of running on the following platforms
  - AIX
  - FreeBSD
  - HP-UX
  - Linux
  - macOS
  - NetBSD
  - OpenBSD
  - Solaris
  - and others
- **Tool should support the following features:**

  - **Security auditing**
  In-depth scanning of systems.

  - **Vulnerability scanning**
  Discovers and solves security weaknesses.

  - **System hardening**
  Improve security defenses by implementing system hardening measures.
- **System areas that are checked:**

- Boot loader files
- Configuration files
- Common files by software packages
- Directories and files related to logging and auditing

- **Tool should support the following test categories:**

-

- accounting
- authentication
- banners
- boot services
- crypto
- databases
- file integrity
- file permissions
- filesystems
- firewalls
- hardening
- hardening tools
- homedirs
- insecure services
- kernel
- kernel hardening
- ldap
- logging
- mac frameworks
- mail messaging
- malware
- memory processes
- nameservices
- networking
- php
- ports packages
- printers spools
- scheduling
- shells
- snmp
- solaris
- squid
- ssh
- storage

- storage nfs
- tcpwrappers
- time
- tooling
- virtualization
- webservers

Annexure F

NTP servers

a. **Enquiry No.: SERC/NBK/NTPS/2018**

b. **Quantity required : 4 Nos**

c. **Technical Specifications**

NTP Server is required for clock synchronization of all clients within Network. It works on the principle of client server model. It is also used to mitigate the variable network latency.

* Physical, Electrical & Operating specifications:

Rack Mountable, Standalone device should have front panel LCD/LED display to show run time. Hardware should have minimum four RJ45 10/100/1000 Base-T Ethernet full duplex NTP outputs

Operating Temperature Range: 0° C to 50° C

Relative Humidity: 0-90%, non-condensing

Operating Voltage Range: 90V-240V

STRATUM 1 compliant (ITU-T G.811) NTP Server with GPS/GLONASS and Stratum 2 on hold over

Rubidium atomic clock or standard oscillator for Lab NTP severs.

NTP server must have three year product warranty. Vendor should provide life time technical support.

NTP server should be able to synchronize min 1000 clients at one time.

NTP server should have battery backup with backup up to 1 month in power down mode

Dual Redundant DC/AC power supply

Leap Second correction support

* Protocols: NTP v2, NTPv3, NTP v4: Compatible Unicast, Broadcast, Multicast, Anycast, Peering, MD5 /SHA1 authentication, SNTPv4, TIME + DAYTIME protocol, > 1000 NTP requests per second.

* Network Communications & Management: Web based GUI, Secure session management using HTTP / HTTPS, SSH v1.3, SSH v1.5 and SSH v2 , SSL/TLS client to web server security, Secure Network Management enable /disable options, RJ45 ports (10/100/1000 Base - T), IPv4, DHCPv4, SMTP, Secure Audit and reporting via SNMP v3 (v1, v2, v2c as well), Alert notification via SNMP trap,

* Security Features: Enabling/disabling protocols, Web based GUI, Role sensitive user interface, Password Protection to GUI, SHA1/ MD5 authentication, SSL encryption, SFTP: Exchange data with an FTP server using an SSH encrypted protocol, SNMP: Configuration and remote settings via an encrypted connection, Logging by Syslog.

* Antenna/ GPS, GLONASS, Signal Receiver:

GPS/GLONASS rooftop pole mount or window mount or Indoor antenna.

Connecting cable length up to 200 meters for outdoor/window mount antenna.

GPS time traceable to UTC (Coordinated Universal Time, ITU)

Power Contact/Lightening Protection for antenna

System should be capable of tracking minimum 3 satellites at a time.

Antenna required GPS/GLONASS signal strength for Tracking /Cold Start > -145bB

Time Accuracy: GPS/GNSS time : ± 1 micro sec

Synchronizing Time : <30 Sec

Oscillator aging (Monthly): ±1×10-7

Holdover Accuracy (per year, ITU T G.812): 1 micro Sec with Rubidium/OCXO, 1 mSec without OCXO

* Compliance specifications

All equipment shall be tested, labeled and certified by a nationally recognized and approved testing laboratory to meet the electromagnetic compliance requirements of India.

* Network Clocks:

The network clocks shall be a high quality, durable, designed for easy, cost effective, and reliable installation and use standard RJ45, 10/100 MB Ethernet style connectors. Clocks shall be deployable within 100 meters cable distance. The time displayed on the

face of the network clocks may either be UTC time or local time and shall be configurable via software.

Accuracy: The networks clock displays shall be accurate to within 50 milliseconds of the UTC time reference provided by the NTP server(s) when synchronized.

Protocol Support: DHCP, SNTP, SNMP

Clock should support Power over Ethernet Technology

* GUI Interface – Windows configuration

The network clock system shall include a GUI (Graphical User Interface) based network software application, operating under the Windows OS, for configuration and maintenance of [the network time server and] all network clocks.

The GUI application shall include password protection of the clock configuration, encrypted communication, and the ability to enable or disable options that might reduce security. A status display to remotely monitor the time displayed on the clock, the internal UTC time, synchronization status, and any error condition regarding the clocks network status shall be provided by the network software.

Annexure G

Spectrum Analysers

a. **Enquiry No.: SERC/NBK/SA/2018**

b. **Quantity required : 1 No**

c. **Technical Specifications**

* Frequency:

1. Frequency range: 10 KHz to 7Ghz

2. Aging per year with OCXO (Oven Controlled Crystal Oscillator): ±1 × 10–6

3. Initial Calibration Accuracy: ±1 × 10–6 Hz

4. Operating Temperature range: 0℃ to 50 ℃, reference 25℃

5. Marker Resolution: Span / (Sweep Points-1): 1Hz

6. Frequency counters resolution: 0.01 Hz

7. Resolution Bandwidths: 1 Hz to 8 MHz

8. Video Bandwidth: 1Hz to 8 MHz

9. Minimum analysis bandwidth: 40MHz

* Amplitude:

10. Displayed average Noise level (DANL): - 145 dBm at < 1 Ghz, -140dBm >1GHz & < 7GHz

Typical DANL (1Hz) RBW = 1 kHz, VBW = 1 Hz Without pre-amp on

11. Phase Noise @ 1Ghz (10 Khz offset): - 110dBc/Hz

12. Amplitude accuracy: ± 0.5 dB or better @2GHz

13. Third Order Intercept TOI : 20dBm at < 8GHz

14. Display Amplitude Range: DANL to +20 dB

(Please provide maximum input level protection)

15. Sweep Time: 1ms - 1000s

16. Number of Points: 100 to 32000

17. Standard attenuator range: 0 - 70 dB

18. Standard attenuator step: 5dB

19. Marker peak search: 5 ms or better

* Applications

20. EMI Pre compliance, Noise figure, Phase noise, Real time spectrum analysis, Base Station Testing, IoT

21. 1xEV-DO, CDMA 2000, CDMA One, 2G, 3G, LTE FDD-TDD, LTE Advanced FDD-TDD, Bluetooth, WLAN (Optional & Future Upgradable)

* General:

22. Support for RF Power Sensors: Device Should Support Power Sensors for Power Measurements, Power Sensors may be directly connected & used for measurements, quote for power sensors with data sheets.

23. Screen size : Minimum 8 Inches

24. Equipment shall provide mouse and key board ports (via USB)

25. Equipment should provide for Log generation (Device should support minimum 32 Gb internal storage) & Screen Shot saving facility. Logs should be exportable to external device. Proprietary software needed for analysis of Logs in external device/computer should be provided by Vendor.

26. Omni Antenna in the operating frequency range of device.

27. Equipment should come with Calibration certificate. Vendor should provide details of tentative recalibration schedule (Calibration Interval) and calibration price

28. Device should be SCPI Language Compatible.

29. Operating Input power supply range 100V-240V

30. Operating Temperature and Humidity range of the device should be mentioned

31. 2 years Warranty and 3 Years AMC

32. Operating Manual / Standard Interface Equipments should be provided

33. Please specify the Input Signal VSWR over the operating frequency range

34. EMI/EMC Compatibility as per existing National /International standards

35. Availability of Test Reports from Central Govt/NABL/ILAC accredited Lab covering all the features & functional requirements.