Comparative study of Cyber Security Assessment Tools

R.Anusooya[1]

[1]*Computer Division, IGCAR, Kalpakkam, Tamil Nadu, India*

Abstract – *Organizations either private corporations or public institutions are facing constant and sophisticated cyber threats and cyber attacks. Many organizations have developed cyber security culture and awareness to safe guard their important data and assets. In order to protect against cyber threats, attacks and challenges, cyber security auditing should become part of the organization's routine activity. However, increased growth and complexity of cyber attacks and convoluted cyber threat landscape, challenges the cyber security audits and putting in evidence the critical need for new cyber security audit tools. This article gives a comparative study of cyber security audit tools and best practices / methodologies to be followed while conducting an information security audit.*

Key Words: Cyber Security, Security Audit, Security assessment tools, Security Audit Tools, Incident management plans, Audit Methodology

1. INTRODUCTION

The higher growth rates observed on the Internet is driven by ever greater amount of online information and knowledge. Commerce, communication, entertainment and Social networking are widely appreciated; information access without authorization is increasing rapidly. Hence, necessity has risen to follow comprehensive methodologies for maintaining availability, confidentiality and integrity (ACI) of information and to secure it. Cyber Security Auditing ensures ACI of Organization's information. The reason behind auditing is identifying the vulnerabilities and repairs them. It ensures policies, procedures and security controls are placed properly and working effectively. New vulnerabilities keep coming on day to day basis in kernel, services, protocols and application packages. These vulnerabilities have to be plugged at the earliest to continue to be secure.

In order to protect against cyber threats, attacks and challenges, cyber security auditing should become part of the organization's routine activity. [1] Organizations should use multiple audit tools for different cyber security aspects with diverse operations and for supporting different levels of users. [2] However, increased growth and complexity of cyber attacks and convoluted cyber threat landscape, challenges the cyber security audits and putting in evidence the critical need for new cyber security audit tools. [1]

To ensure the security of the various servers and systems placed on the network, security has to be assessed through effective security auditing using proper audit tools. This document describes various audit techniques, methodologies and comparison of security audit tools.

2. BEST PRACTICES / METHODOLOGIES OF CYBER SECURITY AUDIT

There are different types of security auditing techniques. Some techniques are human initiated and conducted. Other tests are highly automated. Many excellent tools, freeware and commercial products are available. If the system is complex and highly critical, penetration testing can be deployed to evaluate the security. Overt testing and covert testing are the two methods of penetration testing. How hackers will be using the commonly available tools and methods for accessing an organization's system is the main purpose of penetration testing. Next section describes the best practices and audit methodologies to be followed for improving an Organization security posture.

2.1 Best Practices

Many security tools offer surveys and evaluations to help organizations assess their security posture. These evaluations help to determine the level of vulnerability, identifying risks and weaknesses and prioritize it according to its severity. Certain changes and adjustments to security practices will have a larger effect on organization security posture, so it's important to tackle those first. The following sections elaborate the best practices to be followed while performing security audit [3]

2.1.1 Performing Security assessment

Assessment should always be the first step to improve the security posture. Cyber security risk assessment will help to identify all possible vulnerabilities across all assets, way to exploit it, potential impact of data breach and more. An in-house security team should regularly run this kind of security assessment.

2.1.2 Incident management plan

An incident management plan is a key part of organization's security. Prevention and precautionary measures should be taken against incidents by each and every organization to continue their businesses without any interruption. For this a team (IT security team) should be appointed to take responsibilities in case any incident happens and sort out remediation plans.

2.1.3 Prioritize risks

The IT security team should prioritize the risks and vulnerabilities that their organization facing and immediately fix those vulnerabilities by patching or updating the services. For business continuity, the high priority risks which have largest impact on business should be taken first and plan should be made to fix it, so that time and efforts of IT Teams can be managed more efficiently.

2.1.4 Integrate Security into daily application monitoring

Implementing security testing methods will help integrate security into daily application monitoring by using commercial/in-house developed applications. This application should examine the organization assets for vulnerabilities, identify security gaps, monitor logs and real time app data to detect and remediate attacks as they occur.

2.1.5 Automate threat detection and remediation

Many commercial audit tools are available in the market to find out the threats automatically and give the remediation to overcome those threats.

2.1.6 Regular updation and patch management

IT Security teams should be prepared to make regular changes and adjustments to stay apprised of new advancements in security technology and modern threats. IT security teams should therefore do regular updates, patch management and reassessments to ensure that malicious actors can't take advantage of outdated technologies.

2.2 Audit Methodology

The auditing methodology can be pictorially represented as below, Fig -1. It has three phases.

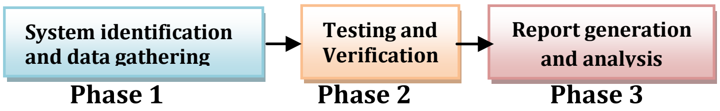
System identification and data gathering
Testing and Verification
Report generation and analysis
Phase 1
Phase 2
Phase 3

Fig – 1 Audit Methodology Phases

Before performing any audit a network security auditor must fully understand the network setup as well as functions or missions supported by the network. This can be accomplished by data gathering and analysis of the network owner's existing documentation. The important aspects like network topology, network protocols, internet connections, server or infrastructure hardware, WAN/extranet connections, operating systems and remote access solutions data/events should be gathered. After identifying any events or occurrences in the system, Alarm or Triggers should be sent to the Administrators for further testing and verification. A report can be generated after analyzing these events and necessary actions should be taken according to that report.

3. AUDIT TOOLS CLASSIFICATION & COMPARISON

Security auditing with proper audit tools plays a vital role in identifying various types of vulnerabilities through different operations. There are wide varieties of security tools available in the market and Internet for conducting Security Audit. Classifications of security audit tools are shown below:

- Network Mapping Tools
- Perimeter Security Tools
- Network/Web Application Vulnerability Scanning Tools
- Operating System Hardening Tools

- Trojan/KeyLogger/Root-kit Analysis Tools

3.1 Network Mapping Tools

Network mapping tools are used for visualizing organization's network devices and for creating maps. It scans all the active devices and identifies the network services, applications and operating system running on those devices. Port scanner part of mapping tools finds all the open UDP and TCP ports. Some tools identify and automatically create network topology/drawing in 3D form.

Visualizing networks, monitoring devices and diagnosing the network are three important functionalities of network mapping tools. The usage or importance of these tools is that it improves the uptime and health of organization's network. Some commonly used tools are Solarwinds Network Topology Mapper, ManageEngine OpManager, Datadog Network Performance Monitoring, Auvik, Paessler PRTG Network Monitor, EdrawMax, NMAP, Cacti, Networkmaps, NagiosXI, OpenNMS, etc.,

Network mapping tool functionality is represented in the following figure, Fig – 2.

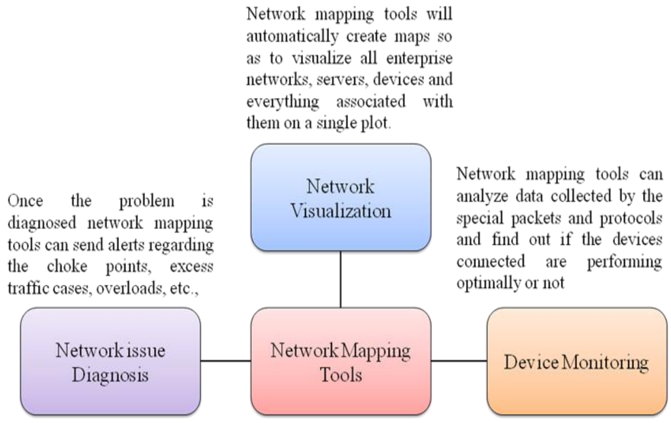
Network mapping tools will automatically create maps so as to visualize all enterprise networks, servers, devices and everything associated with them on a single plot.
Network Visualization
Once the problem is diagnosed network mapping tools can send alerts regarding the choke points, excess traffic cases, overloads, etc.,
Network mapping tools can analyze data collected by the special packets and protocols and find out if the devices connected are performing optimally or not
Network issue Diagnosis
Network Mapping Tools
Device Monitoring

Fig – 2 Network Mapping Tool

3.1.1 Solarwinds Network Topology Mapper

Auto discovery of entire network and builds multiple maps in a single scan. It performs multi-level network discovery. Multi-level Network Discovery is performed with this software. This software is suitable for small to large businesses. Commercial and free trial version of the software is available.

3.1.2 ManageEngine OpManager

OpManager performs real-time network monitoring. Memory, Disk and CPU utilization of servers are monitored. This software is suitable for big enterprises. Commercial/trial version of the software is available.

3.1.3 Paessler PRTG Network Monitor

Monitors and manages Network and Cloud Computing services centrally. Bandwidth utilization of each devices and applications are determined and identifies the source of bottlenecks. It provides detailed statistics of each and every application in the network. This software is suitable for big enterprises. Commercial/trial versions of the software are available.

3.1.4 NMAP

NMAP is an open source software used for Port scanning mechanisms, version detection of application and operating systems. Rapidly scans huge networks with thousands of systems. It supports mapping of different network layers devices.

3.1.5 Networkmaps

It is an open source web based 3D network diagram editor that separates Layer 2 and Layer 3 network diagrams. When users configure devices on the Layer 2 or Layer 3 networks, 3D diagrams of network maps will be created automatically. It can automate network diagrams using API.

3.1.6 OpenNMS

OpenNMS is an open source solution that helps in auto discovery of devices connected in a network. Supports 2nd and 3rd layer network topologies, it generates and sends alerts in case of any network disruption.

The following Table – 1 gives the platform details of Open source and Commercial Network Mapping tools

Table - 1 : Network Mapping tools

Sl. No.	Network Mapping Tool	Platform	Commercial / Opensource
1	Solarwinds Network Topology Mapper	Windows	Commercial / Free trial version is available
2	ManageEngine OpManager	Windows and Linux	Commercial / Free trial version is available
3	Paessler PRTG Network Monitor	Windows	Commercial / Free trial version

			is available
4	NMAP	Mac OS, Windows Linux	Opensource
5	Networkmaps	Mac OS, Windows, Linux	Opensource
6	OpenNMS	Windows, Linux	Opensource

3.2 Perimeter Security Tools

Perimeter Security tools ensure the security of perimeter level devices like Router, Firewall and Switches. Routers are devices designed to provide connectivity between organization's networks to service provider through proper routing. Since the router/firewall represents an entry point into the network, it is important to implement security mechanisms in the router/firewall. Auditors should review router/firewall configuration file for secure configuration as a step for analyzing perimeter security.

This process consists of analyzing the router policy/firewall rule sets of the organization, identify the operating system version and validate that any known vulnerabilities or patches posted by the vendor have been applied. Ensure that adequate filtering is being configured using ACL (access control lists) / Rulesets. Verify that the passwords to all interfaces are set with strong passwords and encrypted. Also ensures that unnecessary network services and interfaces are disabled and improves network devices configuration.

For measuring the security level of perimeter devices, many open source and commercial audit tools are available in the market. Commonly used tools are Router Audit Tool (RAT) from Center for Internet Security (CIS) and Nipper Studio from Titania. Fig-3 shows the perimeter security devices of a typical organization and Table-2 shows the comparison between the two router audit tools, RAT and Nipper Studio.

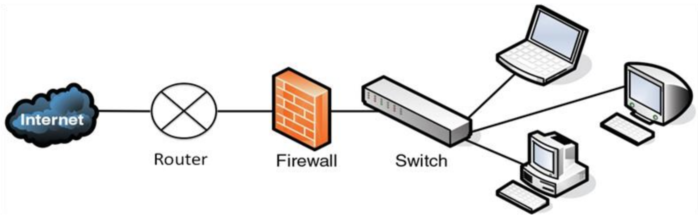

Fig – 2: Perimeter Security devices

Table-2: RAT vs Nipper Studio

Sl No	Features	CIS – Router Audit Tool	Titania Nipper Studio
1	Open Source / Commercial	Free Benchmark Guide	Commercial
2	Network devices support	Cisco, Juniper, Check Point Firewall, Palo Alto, etc.,	Cisco, Juniper, Check Point Firewall, Palo Alto, etc.,
3	Audit Methodology	i. RAT offers best practice solutions for securely configuring Network devices/ Firewall / Switches. ii. It helps to ensure cyber-security standards and strengthens the overall IT infrastructure. iii. Audit offline	i. Analyses the network device configurations and interacts with network infrastructure with a skilled penetration test [4] ii. Prioritize and remediates network risks iii. Greater visibility of vulnerabilities which improves resilience iii. Audit online or offline

3.3 Vulnerability Scanning Tools (Network / Web Application Vulnerability Scanners)

Vulnerability scanners constantly monitor and assess the network or web application servers according to policies and procedures of an organization. It finds out risks and exploits by scanning the network with their updated database of known vulnerabilities. They also provide reports based on the analysis of known vulnerabilities and potential new exploits. Vulnerability scanning deals with the inspection of points of potential exploits to identify security holes. Regular scans detect and classify system weaknesses. These scanners have a high false positive error rate, so only a qualified person/security analyst can assess as well as interpret the results.

For mapping organizations network and identifying open ports network scanners are mainly used. VA scanners identify outdated versions of software, system upgrades and patches. VA scanners detect vulnerabilities and suggest possible remedies. Web Application Vulnerability Scanners helps in the discovery of web-based security holes or problems with authentication credentials, key-based authentication, and credential vaults. It utilizes the database of known vulnerabilities. Vulnerability Scanners can be Host-based or Network-based.

3.3.1 Nessus

Nessus is a network / web application vulnerability assessment scanner used to automate vulnerability detection and subsequently analyze them. It gives the detailed report of old patches, misconfigurations and flaws. It is gives a remediation to identify and fixing those vulnerabilities. It has a wide variety of plug-ins database for finding out the latest security exploits. Many scan templates and pre built policies along with realtime updates are available. Different formats of report can be generated using this tool.

3.3.2 Edgescan

Edgescan is a smart vulnerability management solution for Network and application layers devices. It is used for IOT and API detection. Generates alerts and gives remediation with its report. It prioritize the alerts and gives timely guidance to improve the security posture. API Security Testing, dashboard at one place

3.3.3 Beyond Security-beSecure

Beyond Security-beSecure is a automated vulnerability management solution for an organization. It has the static and dynamic application security testing feature which finds out the run time errors, software vulnerabilities and flaws during the development phase of software life cycle. It can be used for Cloud based systems for finding out the vulnerabilities. It covers internal IT polices requirements and provides the compliance reports.

3.3.4 IBM QRadar

IBM QRadar vulnerability manager is a network scanning platform that detects vulnerabilities within the applications, systems, and devices on your network. Security intelligence feature helps to manage and prioritize network vulnerabilities by continuously monitoring security vulnerabilities, improve resource configuration and identify software patches. Third-party scanners can be integrated with this tool.

3.3.5 Acunetix

Acunetix is a web application vulnerability scanner which can be used for single host or for an entire enterprise network. It can be easily integrated with any opensource tool for testing the web applications using its own API. OWASP's top rated web applications vulnerabilities are easily found out by Acunetix. It generates the customizable reports with low false positive rates.

3.3.6 OpenVAS

OpenVAS identifies and enumerates the vulnerabilities and rank those vulnerabilities present in a system or network in order to patch them. [5]

3.3.7 Nexpose

Nexpose community edition is an opensource vulnerability scanner finds the applications/active services which are running in the system and finds the existing vulnerability associated with them. It supports vulnerability management's lifecycle, including discovery, verification, risk classification, impacts analysis, detection, mitigation and reporting.[6]

3.3.8 Metasploit

Metasploit is one of the best penetration testing frameworks used to find out vulnerabilities in the systems before exploitation by hackers. Various tools, libraries, user interfaces, and modules of Metasploit allow configuring an exploit module, pair with a payload, point at a target, and launch at the target system.

3.3.9 Burpsuite

Burpsuite commercial version is an integrated platform and graphical tool for performing security testing of web applications. It provides a comprehensive solution for web application security checks. It has the following features like proxy server, scanner, intruder, comparer, repeater, decoder, spider, etc., Web traffic between the source and destination can be inspected easily using this tool.

Some of the common vulnerability assessment/scanner tools open source and commercial are mentioned in the below table, Table-3

Table – 3: Network/Web Application Vulnerability Scanners

Sl No	Network Mapping Tool	Platform / Best suitable for
1	Nessus (Commercial)	Windows, Linux, Mac OS, Cloud (SaaS) / Small to large businesses
2.	EdgeScan (Commercial)	Cloud (SaaS) / Small business
3.	beSecure (Commercial)	Cloud (SaaS) / Small to large businesses
4.	IBM Security QRadar (Commercial)	Windows, Mac OS, Cloud (SaaS) / Small to large businesses
5	Acunetix (Commercial)	Linux, Window, Mac OS / Small to large businesses
6	OpenVAS (Open source)	Linux / Small to large businesses
7	Nexpose Community edition (Open source)	Windows, Linux, Private cloud (SaaS) / Small to large businesses
8	Metasploit Framework (Open source)	Linux / Small to medium businesses
9	Burp Suite Community Edition (Trial Version)	Windows, Linux, Mac OS / Small businesses

3.4 Operating System Hardening Tools

Hardening tools are designed to detect vulnerabilities and configuration flaws found in an operating system and computes overall score for security of each system. It does an in-depth audit and needs to be executed on the host system.

3.4.1 CIS-CAT Pro

Center for Internet Security provides tools for benchmarking of systems for security. It is a collection of tools to evaluate all types of operating systems like Linux and Windows. Assessment of vulnerabilities will be done based on the benchmark policies due to missed system patches for Linux and Windows operating systems. Command line or Graphical User Interface (GUI) can be used for performing assessment activities. Supports automated configuration assessments for 80+CIS Benchmarks. [7]

3.4.2 CIS-CAT Lite

CIS-CAT Lite provides detailed assessment of system's conformance with CIS Benchmarks. This tool has a scoring capability and generates report. IT shows the loopholes in OS configuration and gives recommendations to securely configuring the system.

3.4.3 Lynis

Lynis – security tool used for hardening of systems running in Linux or MacOS operating system. It provides host level security based on the OS hardening concepts. It performs health scan of systems to find out if any OS related vulnerabilities are found in the server. Report generates with score in the scale of 1 to 100. Score above 80 indicates that is a good score and the system is hardened well. [8]

3.4.4 OpenSCAP

Open source community develops the configuration baselines and hardening guides for ensuring the security policy of the server and best suits the needs of an organization, regardless of its size. [9]

The following table, Table-4, lists Commercial and Open Source OS hardening tools available in the market.

Table-4: OS Hardening Tools

Sl No	OS Hardening Tool	Platform	Commercial/Free Edition/Opensource
1	CIS-CAT Pro	Windows, Linux, Mac OS	Commercial
2	CIS-CAT Lite	Windows, Linux, Mac OS	Free Edition
3	Lynis	Linux, Mac OS	Open Source
4	OpenSCAP	Linux	Open Source

3.5 Password cracking tools

Password cracking programs are useful for identifying weak passwords. Weak Passwords are the common entry for the attackers; hence strong password should be used in all the systems. Password cracking tools use different methods like dictionary attack, brute force attack, Rainbow table attack, cryptanalysis for recovering passwords [10]

One time password, Encrypted password, Finger print authentication should be used in the Network for improving the security.

3.5.1 CrackStation

CrackStation uses lookup table to crack Password Hashes. Mapping of hash of the password and correct password for that hash is stored in the lookup table. Hash values are indexed for quick search of given hash values. Following protocols like MD and SHA, QubesV3.1BackupDefaults and whirlpool are supported by Crackstation.

3.5.2 Password Cracker

Password Cracker finds out the hidden passwords of windows applications. It supports multiple languages. It cannot restore the password protected document as password encryption is not supported by this tool.

3.5.3 AirCrack-NG

This tool is used for wifi networks. It analyses and cracks the wifi passwords. WPA/WEP passwords are supported by this tool. It cracks the WEP keys using FMS attack.

3.5.4 Rainbow Crack

Rainbow crack is an optimized time-memory trade-off technique tool, uses rainbow tables for cracking password hashes. It supports high compute processing and GPU acceleration. Supports NTLM and LM, MD5 tables, SHA2 tables.

3.5.5 John the Ripper

John the Ripper is used for remote and local password recovery. It auto detects password hash types and mostly used by pentesters for finding out the weak passwords. Supports DES, SHA and MD5 tables.

3.5.6 ophCrack

ophCrack is a opensource program that can crack windows passwords. It supports NT Lan Manager and Lan Manager. Window passwords can be cracked using the rainbow tables on a time-memory trade-off technique.

The following table, Table-5 lists the commonly used password cracking tools.

Table-5: Password Cracking Tools

Sl No	Password cracking Tools	Platform	Commercial / OpenSource
1	CrackStation	Windows, Linux, Mac OS	Open Source
2	Password Cracker	Windows	Open Source
3	AirCrack	Windows, Linux, Mac OS	Open Source
4	Rainbow Crack	Windows, Linux	Open Source
5	John the Ripper	Windows, Linux, Mac OS	Open Source
6	ophCrack	Windows, Linux, Mac OS	Open Source

For different purposes, different password cracking tools are used. Brutus is suitable for recovering hidden passwords in Windows. John the Ripper, CrackStation and ophCrack are suitable for remote password recovery.

3.6 Trojan / Keylogger / Root-kit / Analysis Tool

These analysis tools are used for analyzing any rootkits, keylogger or trojans activities found in the system.

3.6.1 Avast aswMBR

This a rootkit scanner tool from Avast, which scans for MBR/VBR/SRV rootkits. Virtualization is used for detecting stealth rootkits. Some of the common malwares like Sinowal, whistler, SST, Cidox, Zaccess and alureon are detected by this tool. [11]

3.6.2 GMER

GMER scans and analyses the system and detect if any rootkits are present in the system and removes it. It creates a log of hidden processes, threads, modules, services, files, MBR, etc.,

3.6.3 Kaspersky Lab TDSS Killer

This utility is developed by Kaspersky lab to detect and remove TDSS rootkits. It scans for Rootkit.Win32.TDSS, Bootkits, Tidserv, Alureon and attempts to remove it

3.6.4 Malwarebytes Anti-Rootkit

Malwarebytes Anti-Rootkit scans for system drivers, MBR, VBR and system files to find out the rootkit activity and removes it from the system. Rookits are repaired and damage caused by them is rectified using this tool.

3.6.5 Trend Micro Rootkit Buster

This tool scans MBR, Files, Registries, Kernel code patches, processes, services to find out if any rootkits are present in the system and tries to remove it. [12]

3.6.6 UnHackMe

Detects and removes new generation of Trojan programs / invisible Trojans. It scans MBR, Files, Registries, Kernel code patches, processes and services to find out if any rootkits are present in the system and removes it.

3.6.7 Chkrootkit

Chkrootkit is a unix based tool to check the system locally for any known signs of rootkits. It scans for system programs and files for signatures. It checks system binaries for any rootkit modification and reports it.

3.6.8 Rootkit Hunter

This tool is used to find out backdoors and possible local exploits. It scans for files and system programs to detect any known rootkits and malware.
Some of the commonly available tools in the market are mentioned in the following table, Table-6.

Table-6: Trojan / Keylogger / Root-kit / Analysis Tool

Sl No	Rootkit/Anti Trojan Tools	Platform	Commercial / Freeware / Opensource
1	Avast aswMBR	Windows	Freeware
2	GMER	Windows	Freeware
3	Kaspersky Lab TDSS Killer	Windows	Freeware
4	Malwarebytes Anti-Rootkit	Windows, Mac OS	Commercial
5	Trend Micro Rootkit Buster	Windows	Freeware
6	UnHackMe	Windows	Commercial. 30 days trial version is available
7	Chkrootkit	Linux	Opensource
8	Rootkit Hunter	Linux	Opensource

4. CONCLUSIONS

Security Auditing is a continuous process and with good administration, the network and assets can be made fairly secure. An effective and proper utilization of security audit tools will evaluate system security mechanisms and validate that systems are operating according to the organization's security policies and system security requirements. A security auditor can use the above mentioned tools for cyber security auditing and evaluation of their enterprise network security. Most of the tools are user friendly and have proper documentation. System administrators/IT Security teams can make use of these tools for self evaluation and secure their enterprise assets. Hence, with good and effective security assessment tools, IT Teams can evaluate and protect an Organization from cyber threats and attacks.

REFERENCES

[1] Security Management Techniques and Tools for IS Auditing, in the 2019 IEEE, First International Conference of Intelligent Computing and Engineering (ICOICE) by Osamah M.Al-Matari, Iam M.A.Helal, Sherif A.Mazen and Sherif Elhennawy

[2] Cybersecurity Tools for IS Auditing by O. Almatari, I. Helal, S. Mazen, and S. Elhenawy, in the 6th International Conference on Enterprise Systems, Limassol, Cyprus, 2018, p. 8.

[3] https://www.appdynamics.com/blog/security/7-steps -to- strengthen-your-security-posture/, 31/03/2022

[4] Titania Nipper Data Sheet, https://info.titania.com/hubfs/Nipper-US-Datasheet.pdf on 23/03/2022

[5] OpenVAS by Greenbone, https://www.openvas.org/, on 23/03/2022

[6] Nexpose community edition, https://www.javatpoint.com/nexpose on 23/03/2022

[7] https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro, 31/03/2022

[8] https://cisofy.com/lynis/, 31/03/2022

[9] OepnSCAP, https://www.open-scap.org/tools/, 31/03/2022

[10] Password Hacking Tools, https://www.softwaretestinghelp.com/, on 31/03/2022

[11] Avast aswMBR, https://www.avast.com/c-rootkit-scanner-tool, on 31/03/2022

[12] Trendmicro Rootkit Buster, https://www.trendmicro.com, on 31/03/2022

BIOGRAPHIES

R.Anusooya received her B.E Degree from Madras University, T.N in 1997. She joined in Indira Gandhi Centre for Atomic Research (IGCAR) in 2001. She did her M.Tech in Sathyabama University in 2013. She is currently a Scientific Officer-F in Electronics and Instrumentation Group, IGCAR. She has 8 Journal Publications / Conference Papers and 25 Internal Design Reports.