IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Comprehensive Review on Cyber Security Tools to Handle Vulnerabilities

Dr Manjula K, Bhoomika K S, Raksha K, Harshini J P

Associate Professor, Global Academy of Technology, Bangalore, Karnataka, India

Student, Global Academy of Technology, Bangalore, Karnataka, India

ABSTRACT: The internet has today become a very important instrument in our daily lives. It is constantly growing and offers boundless materials that may be accessed without restriction. According to current figures, India has 833.7 million internet users, which places it second in the globe. And hence it has become clear in recent years that nobody is safe from the threat of cybercrime. Cybercrimes can be committed by both individuals and groups of people. Importantly, disclosing personal information may have unfavourable effects. It frequently causes business difficulties, legal repercussions, and occasionally even financial loss. Therefore, it is crucial for enterprises to maintain a strong security posture, and it is crucial to take preventative actions to shield ourselves from security threats and cyberattacks. Cybersecurity is a crucial component that aids in protecting systems from such viral attacks in addition to helping to secure information. Vulnerability management is essentially an automated procedure that protects company applications, networks, and computer systems from hacker attacks and data breaches. Companies utilize a variety of tools, techniques, and a few sophisticated methodologies to guard their systems and networks against unauthorized access. By adopting these solutions, organizations can better defend their data and IT infrastructure from online threats. This study therefore provides an exhaustive review about the application of cyber security tools, with a view to making it easier for students, researchers and academicians to explore into cyber security field.

KEYWORDS: Cyber security, threat, cyber attack, vulnerabilities, cyber tools.

I. INTRODUCTION

In the context of networking, cybersecurity refers to the activity of defending computer networks, systems, and data against online dangers and illegal access. It includes a variety of methods, procedures, and tools intended to protect the availability, confidentiality, and integrity of data transferred through networks. Creating a secure environment that protects sensitive data and prevent cyberattacks is the aim of cybersecurity in networking. The use of the internet and other digital gadgets has increased significantly in recent years, and as a result, we have cyber-attacks. The reason for this is that students and researchers are particularly vulnerable to these threats since they depend on the internet and devices for educational and recreational activities. Let's quickly review the evolution of the internet. The illustration in Fig 1provides a cursory overview of how the internet has changed.The US Department of Defence (DOD) established the network known as ARPANET (Advanced Research Projects Agency Network), also known as the "granddad" of the Internet in the early 1960s saw the beginning of the network's construction, and DOD financed significant research that led to the creation of the first protocols, languages, and frameworks for network communication. ARPANET was mostly used for academic and research purposes. Since the ARPANET is regarded as the precursor to the current internet, many of the protocols used by computer networks today were created for it. **[3]**

Internet service providers found PSINet, UUNET, Netcom.

Fig 1 Evolution of Internet

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Then the National Science Foundation (NSF) awarded funding to create the Computer Science Network (CSNET) in 1981 so that all university computer scientists may benefit from networking services. In 1985, NSF thought about how it could make its freshly built supercomputer centres advanced computing power more accessible. Any workable solution had to connect numerous research universities to the centres since NSF intended for scientists and engineers around the nation to share the supercomputers.**[5]** The transition to the modern Internet began with the invention of the World Wide Web, which led to a sustained exponential growth as successive generations of institutional, personal, and mobile computers were connected to the network. Although academics used the Internet extensively in the 1980s, it was subsequent commercialization that brought its services and technologies into almost every facet of modern life. Through instant messaging, Internet forums, and social networking sites, the Internet has facilitated and accelerated the development of new kinds of interpersonal communication. For huge merchants, small businesses, and entrepreneurs, internet purchasing has increased dramatically because it allows enterprises to expand their "brick and mortar" presence to serve a larger market or even sell products and services wholly online**.[4][6]**

1.1 Internet Protocols:

Network protocols are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely, the current section discusses about the protocols that helps in the communication and data exchange across the network of the devices.

Protocols play a crucial role in enabling the seamless functioning of today's interconnected digital world. Across computer networks, data is communicated, received, and processed according to a set of rules and standards called network protocols. They offer a standardized method of communication for gadgets and systems, assuring accurate and effective data sharing. Aspects of communication that are defined by protocols include data formatting, error management, addressing, and authentication.**[7]** Some of the most widely used network protocols are: 1.TCP /IP: It is the backbone of the contemporary internet. It consists of a group of protocols that let devices to communicate with one another through the internet. IP (Internet

II. RELATED WORK

The first virus, it was Bob Thomas, a developer in ARPANET developed the Creeper software in 1971, which is frequently referred to as the first virus. Creeper was initially created as a security test to determine whether it was possible to create a self-replicating program. It published the message "I'm the creeper; catch me if you can." Since the experiment was risk-free, we can now recognize that it was the first computer worm [is a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems. Computer viruses can be categorized based on attacks on various elements of the system and is capable of putting the system and the data present in the system in danger. Now let us have an overview of the types of computer viruses. Starting with, 1. Boot sector viruses: It infects the storage media on which the operating system is stored and which is basically used to start the computer system. On hard drives and floppy disks, the whole data and program are kept in units known as sectors. The Master Boot Record (MBR) is located in the first sector, designated as BOOT. The purpose of the MBR is to read and load the operating system, allowing the computer to boot up using the OS. Therefore, if a virus assaults an MBR or infects a disk's boot record, the victim's hard drive will become infected when the system is restarted while the infected disk is in the drive. All of the floppy diskettes being utilized in the system will become infected after the victim's hard drive has been compromised. When shared infected disks and pirated software are utilized, boot sector viruses frequently spread to other systems.2.Program viruses: These viruses are active when the program files are executed. Typically, program files with these extensions are: .bin, .com, .exe. After infecting these software files, the virus replicates and spreads to the other programs on the computer system. 3. Multipartite viruses: This type of virus is a cross between a boot sector and software virus. When the infected program is running, it also corrupts the boot record in addition to the program files. The local drive and other programs on the victim's computer system will be infected the next time the victim starts it.4. Stealth viruses: These are difficult to identify because they conceal themselves through camouflaging or masking. They can conceal itself in a way that antivirus software is unable to recognize, preventing proliferation throughout computer systems. To avoid detection, it changes its size and hides in computer memory. Brain was the first known stealth virus to target IBM PCs. A decent antivirus checks the regions the virus must infect by leaving evidence memory to find stealth viruses hiding on the victim's machine. 5.Polymorphic viruses: When a polymorphic virus travels across the system (i.e., multiplies and is hard to detect with the aid of an antivirus

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

tool), it behaves like a "chameleon" and alters its virus signature (i.e., binary pattern). Routines (i.e., tiny programs) of the polymorphic generate can be linked with the current viruses. These generators don't actually create viruses; instead, they do so in order to mask real viruses with morphism. The mutation engine, the first general-purpose polymorphism generator, was published in 1991. Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Engine (DGME), Dark Mutation Engine (DSME), Guns'n'Roses Polymorphic (GPE), and Slayer Confusion Engine (DSCE) are further polymorphic generators that are well-known.6. Macroviruses: Applications that enable MACRO (i.e., macro languages) include Microsoft Word and Excel. These are inserted in the paper as a coded macro. Once the macro virus is installed on the victim's computer, any document that person produces will be contaminated. This kind of virus is somewhat fresh and might have gotten into his or her system.7. Active X and Java Control: The settings for Active X and Java Controls are available in all web browsers. Little knowledge is required to manage and control these web browser settings, which invites threats for the computer system to be targeted by unwanted software(s) floating in cyberspace. These settings include enabling or disabling pop-ups, downloading files, and sound**.[1]**

2.1 Vulnerabilities

Vulnerabilities are slackness or defects in systems, networks, software, hardware, or other components that an attacker could use to compromise the security of those systems. These flaws, which can be inadvertent design, implementation, or configuration issues, give malicious actors the chance to gain access without authorization, damage property, steal data, or disrupt services. Maintaining the security and integrity of digital systems requires identifying and fixing vulnerabilities. The different categories of vulnerabilities is as: i) Software faults: It can be used to obtain unauthorized access or carry out malevolent deeds are known as software vulnerabilities. ii) Hardware flaws: These are security holes in hardware that can be used to compromise a system's integrity.iii) Network vulnerabilities are holes in the infrastructure of the network that could let intruders or other bad actors to access the system or intercept data.

iv) Configuration Vulnerabilities: Systems that are incorrectly configured can reveal security holes that attackers can take advantage of. Common flaws and Exposures (CVE): CVE is a standardized system for locating and naming software and hardware flaws. It is simpler to manage and share information about vulnerabilities across many systems because each vulnerability is given a special identity. A zero-day vulnerability is a security hole that is used by attackers prior to the software vendor being aware of it or having the opportunity to issue a fix. Defenders have no time to get ready because there are "zero days" between the time the vulnerability is found and the attack. Exploits: An exploit is a piece of code or a method that compromises a system by taking advantage of a specific vulnerability. Exploits are used by hackers to enter restricted areas, run malicious software, and carry out other nefarious tasks. Patch and Update Management: To address known vulnerabilities, software makers offer patches and updates. Updating software is essential to reducing the dangers brought on by known vulnerabilities. Security Assessments: To find system flaws before attackers can take advantage of them, organizations carry out security assessments including penetration testing and vulnerability scanning. Threat actors are those who deliberately look for weaknesses to exploit for monetary gain, espionage, disruption, or other harmful goals. These actors include cyber criminals, hackers, state-sponsored organizations, and other malevolent individuals or groups.

2.1.1 Strategies for Mitigation:

To reduce vulnerabilities the strategies that can be employed are is to update firmware and software frequently with security fixes. Employ reliable authentication methods and access controls. Use security best practices, such as secure code and input validation. To find and stop assaults, use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Conduct routine audits and security assessments. Defence in Depth: By making it more difficult for attackers to exploit vulnerabilities, using many levels of security measures, also known as defence in depth, helps to lessen the effect of vulnerabilities. Vendor Response: To appropriately disclose and address vulnerabilities, organizations and software suppliers work together. Patches and advisories are frequently released by vendors to assist users in securing their systems. Ethical hacking: Also referred to as white hat hackers, ethical hackers deliberately look for security flaws in order to assist organizations in identifying and resolving them before nefarious actors may take advantage of them. In the rapidly evolving landscape of cybersecurity, identifying and addressing vulnerabilities is an ongoing process that requires vigilance, proactive measures, and a commitment to maintaining the security of digital systems.We now have a basic understanding of the rise of networks and cybercrime. Cybercrimes thus frequently occur if a system is given an illegal access. Any level of your business could potentially present a cyber risk. Workplaces must offer cybersecurity awareness training to staff members to inform them of typical cyberthreats including social

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

engineering fraud, phishing, ransomware attacks and other malware intended to steal confidential information. Because it guards against theft and loss of all types of data, therefore cybersecurity is crucial. If cyber security specialists didn't constantly try to thwart denial-of-service attacks, it would be practically impossible to use many websites. Your company cannot protect itself against data breach operations without a cybersecurity program, making it an inevitable target for hackers. As a result of increased global connection and the use of cloud services like Amazon Web Services to hold confidential and sensitive data, both inherent risk and residual risk are rising.**[2]** Cyber security is most simply described as a characteristic that protects against online attacks on a company, its personnel, and its assets. Confidentiality. Integrity, and Availability are crucial components of cyber security. Confidentiality focuses on preventing unauthorized access to sensitive information. This principle ensures that only authorized individuals or entities can access and view sensitive data. Confidentiality is crucial for protecting personal, financial, proprietary, and classified information from falling into the wrong hands. Methods used to achieve confidentiality include encryption, access controls, user authentication, and data classification. Integrity ensures that data remains accurate, consistent, and trustworthy throughout its lifecycle. This principle prevents unauthorized modification, alteration, or deletion of data. Maintaining data integrity is vital to prevent data corruption, unauthorized tampering, or unintentional changes that could compromise the reliability and trustworthiness of information. Techniques such as digital signatures, checksums, and access controls are used to safeguard data integrity. Availability ensures that information and systems are accessible and functional when needed. It guarantees that authorized users can access data and resources without excessive downtime or disruptions. Attacks or incidents that compromise availability, such as denial-of-service attacks or system failures, can have significant consequences for organizations, especially those that rely heavily on their digital infrastructure. Redundancy, fault tolerance, disaster recovery planning, and system monitoring are some measures used to maintain availability. These three principles are interconnected, and a balance must be maintained between them. For example, implementing strong security measures for confidentiality and integrity might inadvertently impact availability. Finding the right trade-offs is essential to ensure that security measures do not overly hinder user access and system functionality Additionally, the CIA triad serves as a foundation for broader information security considerations, such as accountability, non-repudiation (preventing parties from denying their actions), and authenticity. Organizations use these principles as a framework to assess risks, design security policies, implement technical controls, and respond to security incidents. By prioritizing and addressing confidentiality, integrity, and availability, organizations can build a strong foundation for maintaining the security and reliability of their systems and data.**[9]**

Fig2: Common model of security systems

The work in this paper is divided in two stages. 1) Text- Detection 2) Inpainting. Text detection is done by applying morphological open-close and close-open filters and combines the images. Thereafter, gradient is applied to detect the edges followed by thresholding and morphological dilation, erosion operation. Then, connected component labelling is performed to label each object separately. Finally, the set of selection criteria is applied to filter out non text regions. After text detection, text inpainting is accomplished by using exemplar based Inpainting algorithm.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. METHODOLOGY

Endpoint security products are created to safeguard a network's endpoints, including laptops, desktop computers, and mobile devices, from potential dangers.

The best endpoint security tools for 2023 include Avast Business Security, ESET Endpoint Protection Advanced Cloud, Trend Micro Worry-Free Services Suites, ManageEngine Vulnerability Manager Plus, ESET Endpoint Security, Trend Micro Apex One, Symantec Endpoint Detection and Response, CrowdStrike Falcon Insight and Cybereason Total Enterprise Protection. We can monitor endpoint security and defend against potential threats with the aid of these tools.

- CrowdStrike Falcon: CrowdStrike Falcon is a cloud-native endpoint security product that combines threat intelligence2, managed threat hunting, next-generation antivirus, endpoint detection and response (EDR), and IT hygiene.
- Symantec Endpoint Security: This program offers cutting-edge threat detection, prevention, and response capabilities to safeguard endpoints from both known and unidentified threats.
- ESET Endpoint Security: This program offers thorough endpoint defence against viruses, phishing scams, ransomware, and other internet dangers.
- Antivirus/Antimalware: Scan individual devices for harmful software, remove it, or quarantine it.

Host-based Intrusion Detection Systems (HIDS): Keep an eye on individual devices and look for odd behaviour. Control which programs are allowed to operate on a device with the use of application white listing and blacklisting. Prevent illegal data transfers or leaks from endpoints with data loss prevention (DLP).**[12]**

3.1 Vulnerability Management Tools

Identify, evaluate, and rank system and application vulnerabilities. Automate the process of installing security updates and fixes with patch management. Tools for managing vulnerabilities are security programs that scan corporate networks for flaws that hackers could exploit. These tools are created to handle network attacks as they happen. The majority of vulnerability management products have functions like asset discovery, vulnerability assessment, vulnerability intelligence, web scanning, automated scans, risk management, risk-prioritization, configuration monitoring, vulnerability scanning, and reporting as well as other more generic aspects.

Top vulnerability management tools for 2023 include GFI Languard , Astra Pentest ,Snyk's Developer Security Platform, Saltstack vulnerability management platform, Skybox Security, Tenable Nessus, Action1, Qualys VMDR 2.0 with TruRisk,owasp and Lacework Cloud Security Platform. The websites https://who.is/ and http://Netcraft.com are used to handle system and application vulnerabilities.

- GFI Languard: In order to maintain the security of all endpoints, GFI Languard has the capacity to identify every device connected to a network, identify any security holes or vulnerabilities in the operating systems, web browsers, and third-party applications, and then automatically apply fixes to every device.
- Astra Pentest: It is a comprehensive platform with a vulnerability management dashboard, manual pentesting options, and an automated vulnerability scanner that may help you automate every stage of the pen test process.
- Saltstack vulnerability management platform: The closed-loop, event-driven automation for ongoing system compliance and vulnerability mitigation is provided by the Saltstack vulnerability management platform.**[13]**

IV. EXPERIMENTAL RESULTS

Mobile device security is the protection of confidential data and information stored on and transmitted through mobile devices such as smartphones, tablets, laptops, wearable, and portable devices.

Manage and protect mobile devices inside of an enterprise via mobile device management (MDM).

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Manage and protect mobile applications with mobile application management (MAM). Top mobile device security tools for 2023 include Belarc, Lynis and CIS CATLIVE v3.

- Penetrate Pro: A penetrating tool with a lot of power. This program will assist you in obtaining the key needed to access the majority of Wi-Fi networks that are now available.
- FaceNiff : This clever program enables sniffing and can record web sessions over the specific Wi-Fi to which your device is connected.

SL.NO	NAME	DESCRIPTON	URL
1.	Mobile Device Management (MDM)	In an enterprise, control and secure mobile devices.	https://www.hexnode.com
2.	Mobile Application Management (MAM)	Organize and protect mobile applications.	https://www.hexnode.com
3.	Belarc	Enables users to use a single database and Intranet service to simplify and automate the management of all of their desktops, servers, and laptops around the world.	https://www.belarc.com
4.	Lynis	A tried-and-true security utility for Linux, macOS, and Unix-based computers is called Lynis.	https://cisofy.com
5.	CIS CATLIVE v3	The free evaluation tool created by the CIS (Center for Internet Security, Inc.) is called CIS-CAT. Users can develop secure settings for numerous technologies with the aid of CIS-CAT.	https://learn.cisecurity.org

V. CONCLUSION

Computer viruses have been a part of our culture for more than 60 years, but what started off as simple cyber vandalism has quickly evolved into cyber crime. Trojans, viruses, and worms are all changing. Hackers are driven and intelligent individuals who are constantly willing to test the limits of connection and coding to create novel infection techniques. PoS (point of sale) intrusions appear to be a growing trend in cyber crime, and the latest Moker remote access Trojan may be a good indicator of things to come. This recently discovered malware avoids all existing safeguards and is challenging to detect and remove. Change is the lifeblood of both attack and defence; thus, nothing is certain. In the modern digital landscape, cyber crimes have emerged as a significant threat to individuals, organizations, and even nations. This paper has explored various aspects of cyber crimes, ranging from their definitions and classifications to the motives and methods of cyber criminals. These activities not only lead to financial losses but also erode trust, compromise privacy, and disrupt the critical infrastructure that underpins our interconnected world. In the realm of today's interconnected digital landscape, cybersecurity tools have emerged as indispensable defenders against an ever-evolving array of threats. This paper has explored a diverse array of cybersecurity tools, each designed to address specific vulnerabilities and mitigate risks across various domains. From network security solutions fortifying our virtual boundaries to endpoint protection tools safeguarding individual devices, these tools collectively form a critical line of defence against cyber attacks. As we conclude this survey, it becomes evident that cybersecurity tools are not just technological components but integral elements of a comprehensive security strategy. They empower organizations to detect, prevent, and respond to threats effectively, contributing to the overall resilience of digital systems. The wide

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

range of tools available, from intrusion detection systems to encryption solutions, underscores the need for a multi-layered approach to security, tailored to the unique challenges and requirements of each context.

REFERENCES

[1] Nina Godbole, Sunit Belapur, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Publications, April, 2011
[2] Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And LegalPerspectives", Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013.
[3] Roberts, Larry. "The Arpanet and computer networks." In A history of personal workstations, pp. 141-172. 1988.
[4] Abbate, Janet Ellen. From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966-1988. University of Pennsylvania, 1994.
[5] Rajiv C. Shah Ph.D.Jay P. Kesan Ph.D.. (2007) The Privatization of the Internet's Backbone Network. Journal of Broadcasting & Electronic Media 51:1, pages 93-109.
[6] Curran, James. "Rethinking internet history." Misunderstanding the internet (2012): 34-65.
[7] A. Segall, "Distributed network protocols," in IEEE Transactions on Information Theory, vol. 29, no. 1, pp. 23-35, January 1983, doi: 10.1109/TIT.1983.1056620
[8] Wei, Pan, Zhiguo Hong, and Minyong Shi. "Performance analysis of HTTP and FTP based on OPNET." In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), pp. 1-4. IEEE, 2016.
[9] Chowdhury, MD Minhaz, Nafiz Rifat, Mostofa Ahsan, Shadman Latif, Rahul Gomes, and Md Saifur Rahman. "ChatGPT: A Threat Against the CIA Triad of Cyber Security." In 2023 IEEE International Conference on Electro Information Technology (eIT), pp. 1-6. IEEE, 2023.
[10]Cyber Security: Understanding Cyber Crimes, computer perspectives and legal forensics (2011)- Sunit belapure Nina Godbole
[11] S. B. Vyshnavi, S. R. Sree and N. Jayapandian, "Network Security Tools and Applications in Research Perspective," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 655-659, doi: 10.1109/I-SMAC47947.2019.9032526.
[12] M. Saleh, N. B. Al Barghuthi, K. Alawadhi, F. Sallal and A. Ferrah, "Streamlining "smart grid end point devices" vulnerability testing using single board computer," 2018 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, Sharjah, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/ICASET.2018.8376802.
[13]M. Walkowski, M. Biskup, A. Szewczyk, J. Oko and S. Sujecki, "Container Based Analysis Tool for Vulnerability Prioritization in Cyber Security Systems," 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 2019, pp. 1-4, doi: 10.1109/ICTON.2019.8840441.
[14]Gerard Johansen, Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response , Packt Publishing, 2022.
[15] M. A. Kunda and I. Alsmadi, "Practical web security testing: Evolution of web application modules and open source testing tools," 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), San Antonio, TX, USA, 2022, pp. 152-155, doi: 10.1109/IDSTA55301.2022.9923130.
[16] S. Vashisht, S. Gupta, D. Singh and A. Mudgal, "Emerging threats in mobile communication system," 2016 [15] International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 2016, pp. 41-44, doi: 10.1109/ICICCS.2016.7542341.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details