SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

CRITICAL ANALYSIS OF PENETRATION TESTING PROCESS AND TOOLS

Geetanjali sao[1*], Sakshi Kumar[2], Dr. Suman Madan[3]
[1,2]*Research scholar, Jagan Institute of Management Studies, Sector-5 , Rohini, Delhi-85,India.*
[3]*Associate Professor, Jagan Institute of Management Studies, Sector-5 , Rohini, Delhi-85,India.*

[*]***Corresponding Author: Geetanjali sao***

Article DOI: https://doi.org/10.36713/epra8540
DOI No: 10.36713/epra8540

ABSTRACT

Information is more susciptible than ever, and each technology advancement creates a new security issue that necessitates a new approach to solving the problem. Penetration testing is used to assess the security of an IT infrastructure by exposing its vulnerabilities in a safe manner. It also aids in acquiring access to the effectiveness of existing defense systems, tactics, and policies. The Penetration testing is carried out on a regular basis in order to detect and control risks to achieve ethics to be possessed by the testing crew involved in penetration test. This research uses a qualitative research methodology for investigating manual testing and automated testing. It further aims at critically investigation penetration testing and its importance with tools available for it.

KEYWORDS: *IT Security, Penetration test, IT governance, Vulnerability assessment.*

1. INTRODUCTION

The all-inclusive nature of testing employed in penetration higher level of protection. In this research paper, we highlighted the relevance of testing aspects and components evaluated during penetration testing, as well as the tools and techniques utilized and the function of penetration testing in the security industry. implementation of IT governance in a company and finally the expert testing adds to the process vey complex. For the course of the test, this process necessitates teams of highly skilled testers. As a result , it is a highly costly choice. These testers must be very experienced because they must control all tasks manually. on the other hand, automated testing is a secure and convenient solution to complete all the penetration testing activates. Additionally, because most operations are automated, the test may take less time than manual testing. The test's simplicity of reproducibility is also a significant advantage over manual testing tailored method. Table 1 provides comparative analysis of manual testing with automated testing on parameters like the process, vulnerability, report generation etc.

The security dangers for corporations, organization, and entities that work with sensitive data from the public sector or not are more than obvious. In many situation these companies and businesses are unable to comprehend the complexity of the actual communication system and have little or no control over it. To have a competitive advantages, all businesses must protect their information. Standard procedures and well documented organized methods are used to protect data. It is also verified that they adhere to secure its requirements and standards. security assurances, For security, proof of accuracy, and penetration tests, a software engineering environment is required processes in regulation.

Penetrating an organization's computing foundation, which comprises hardware, software, and people, is a process. This procedure entails a comprehensive examination of the entire company. In order to discover the weakness, the computing system searches for vulnerabilities such as system configuration software and hardware errors, as well as the operational process . Penetration testing can be used in various segments:

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

1.**Based on the Testing Service :**

- Network penetration test: A Network penetration testing, it helps to identify vulnerabilities within a network. Its one among a number of approaches for preventing illegal network commands.
- Web application penetration testing: A Web application penetration test, looks for any security issues that might have arisen as a result of insecure development, design or coding, to identify potential vulnerabilities in websites and web applications, including CMR, extranets and internally developed programs- which could lead to exposure of personal data, credit card information etc.
- Mobile application: A Mobile application penetration test emulates an attack specifically targeting a custom mobile application and aims to enumerate all vulnerabilities within app.
- Social engineering: A social engineering pen test will help assess and understand the susceptibility within organization to human manipulation via email, phone, media drops, physical access, social media mining etc.
- Wireless penetration testing: a wireless penetration test is comparable to a wired penetration test in that it examines your network using the same methodology.

2. **On the basis of deployment mode**

- Cloud: A simulated cyber-attack on a system housed on a cloud provider, such as Amazon web services(AWS) or Microsoft azure, is known as cloud penetration testing. A cloud penetration tests primary purpose is to identify a system'\s vulnerabilities and strengths.

3. **Based on the vertical industrialization**

- Banking, financial services, and insurance (BFSI): Penetration rate indicates the level of development of insurance sector in a country. Penetration rate is measured as the ratio of premium underwritten in a particular year to the GDP.
- IT and telecom: Mobile Phone Penetration refers to the number of SIM cards or mobile phone number in a certain country.
- Healthcare: Hospital palliative care penetration rates are calculated by dividing palliative care service utilization by the total inpatient population.
- Retail: Market penetration is a measure of how much a product or service is being used by customers compared to the total estimated market for that product or service.
- Government and defense: The Government Accountability Office's report on the cyber security of the department of defense's weapon system revealed chronic challenges.

A security test determines how difficult it is for an attacker to breach an organization's computer network, whereas a PEN test determines how difficult it is for an attacker to breach an organization's computing network. A user demonstrates an unauthorized attack on the test target system by utilizing automatic programmed tools, manual tools, or both.

Table 1. Comparison of manual vs. automated testing

	MANUAL	AUTOMATED
Testing Process	• Manual, non-standard process Labour and capital intensive, • High cost of customization	• Fast, standard process Easily repeatable tests
Vulnerability/Attack Database Management	• Maintenance of database is manual. • Need to rely on public database • Need to re-write attack code for functioning across different platforms	• Attack database is maintained and updated. • • Attack codes are written for a variety of platforms
Reporting	• Requires collecting the data manually.	• Reports are automated and customized.
Clean up	• The tester has to manually undo the changes to the system every time vulnerabilities found.	• Automated testing products offer clean-up solutions
Training	• Testers need to learn non-standard ways of testing. • Training can be customized and is time consuming.	• Training for automated tools is easier than manual testing.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

Lam K, LeBlanc D, Smith BI (2004) discussed that the number of studies have been designed and implemented to help improve the situation of security in data, system and networks. There are several open source scanning tools for security.[1]

McGraw, G. (2006) discussed that the penetration testing helps adherent the audit regulatory standards like PCI DSS, HIPAA and GLBA. This avoids the huge fines for non-compliance.[6]

Arkin, B., Stender, S., and McGraw, G. (2005) discussed in this paper focuses on the power of combining multiple data points to achieve as much visibility as possible within an enterprise. attackers and defenders both have vast toolboxes.[7]

P. Ami and A. Hasan.(2012) Vulnerability assessment and penetration testing were contrasted by the authors. vulnerability assessment is a proactive and methodical approach to identifying vulnerabilities. It is used to find previously unknown faults in a system. From a compliance standpoint, it is also required by industry standards such as DSS PCI. Penetration testing assesses a computer system or network by simulating an attack. It's a method for assessing security that's both proactive and systematic. Vulnerability scans and vulnerability assessments look for known flaws in systems. A penetration test is an attempt to aggressively exploit a system's flaws. While a vulnerability assessment can be automated, a penetration test necessitates a variety of skills.

Zaher Al Shebli, H. and Beheshti, B. (2018) the purpose of this paper is to cover penetration testing, variables to consider when conducting a penetration test, the process of conducting a penetration test, and Penetration testing tools and software are routinely utilised. [8]

Mainka C, Somorovsky J, Schwenk J (2012) XML-based SOAP web services are a widely used technology, which allows the users to execute remote operations and transport arbitrary data. It is currently adapted in service oriented Architectures, cloud interfaces, management of federated identities, e Government, or military services.[9]

Table 2 shows the summary of literature survey done.

Table 2: Related Work Summary

AUTHOR NAME	DESCRIPTION	ADVANTAGES/DISADVANTAGES
Lam K, LeBlanc D, Smith BI (2004)	The pen tests become are several open source scanning tools for security.	Flatbed scanners are very accurate and can produce reasonably high quality images./ images produced the scanner can take up a lot of memory space.
McGraw, G. (2006)	The penetration testing helps adherent the audit regulatory standards like PCI DSS, HIPAA and GLBA. This avoids the huge fines for non-compliance.	HIPAA: It increases personal privacy in healthcare information and decision-making. / It increased the administrative requirements of medical care.
Arkin, B., Stender, S., and McGraw, G. (2005)	The Author discuss in this paper focuses on the power of combining multiple data points to achieve as much visibility as possible within an enterprise. attackers and defenders both have vast toolboxes.	Existing Administrative data collection, useful for measuring high-level outcomes / Not always intended for research puposes, can be difficult to access, analysis can be complex.
P. Ami and A. Hasan.(2012)	Vulnerability assessment and penetration testing were contrasted by the authors	Vulnerability assessment: Identify vulnerabilities before cyber criminals do, Save time and money / Make the most of vulnerability scanning, false positives Penetration testing: Penetration testing can identify a range of vulnerabilities, Reports will provide specific advice / If

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

		tester not done right, penetration testing can create a lot of damage.
Zaher Al Shebli, H. and Beheshti, B. (2018)	Penetration test, elements to consider when conducting a penetration test, the process of doing a penetration test, and Penetration testing tools and software are routinely utilized are all discussed.	Manual, testing process is non-standard process Labor and capital intensive, High cost of customization. / Automated, testing process is Fast, standard process easily repeatable test.
Mainka C, Somorovsky J, Schwenk J (2012)	XML-based SOAP web services are a widely used technology, which allows the users to execute remote operations and transport arbitrary data.	Can be leveraged upon existing on-premise implementation within ABC company / vetex services and data, needs re-deployment, to eliminate oracle hosting dependency.

2. PENETRATION TESTING

Penetration testing also aids in the development of essential components of information security strategy by swiftly and accurately finding weaknesses. It also aids in the enhancement of test settings in order to proactively minimize identified hazards. It aids businesses in assessing the consequences and likelihood of vulnerabilities. As a result, the business can set priorities and carry out the mitigation plan.

It protects enterprises from failure by reducing financial loss and ensuring compliance with industry, customers, and shareholders, as well as assisting in the development of trust, corporate image, and the rationalization of IT security investments. Because penetration testing is a proactive procedure, it delivers unquestionable data that aids the firm in meeting regulatory auditing and compliance requirements.

A structured penetration test is performed to identify the risks that may exist if an attacker gains access to a computer system or network of an organization. A PEN test can be used to estimate the migration plan for closing security weaknesses before an actual attack occurs. A pen test aids enterprise in reducing financial and information loss that would otherwise result in a loss of client trust.

2.1 Need for Penetration Testing

Penetration testing has a slew of advantages for business as well as technical perspective. The following are some of the most important reasons to use penetration testing

a) **Security Issues:** Malware attack, network infiltration, and data theft are all examples of security vulnerabilities that can cause service interruptions and unreliable system processes. This may result in as loss of consumer loyalty and have an impact on the company market value. Penetrating testing can help to prevent such incidents by identifying both persistent

b) **Protect Information:** Access control measures, firewalls, cryptography, intrusion detection systems, and other security procedures are used by businesses to protect information. However, with new threats being discovered on a daily basis, it is difficult to maintain constant protection of user system information. By simulating a range of attacks at the same time, penetration testing could address these problems.

c) **Prioritize security risks:** Penetration testing as a regular security practice not only aids in the understanding of security vulnerabilities, but it also aids in the prioritization of these issue. The severity of the concerns discovered during the testing can be prioritised. These initiatives may also result in more efficient budgeting for information challenges.

d) **Financial Loss:** penetration testing can assist you avoid losing money due to service outages caused by malicious assaults. It can also help to avoid or decrease fees from security- related lawsuits.

2.2 Penetration Testing Methodology

Penetration testing should be included as a standard process within the security testing roadmap. Traditionally, organizations prefer to perform penetration testing prior to a product release or a major upgrade. However, it is also advisable to conduct this testing in the following situations:

- New infrastructure is added
- System updates are applied
- Security patches are applied
- User policies are modified.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

The procedure entails a thorough examination of the system for any potential vulnerabilities that may arise as a result of insufficient or inappropriate system configuration, as well as known and undiscovered hardware or software processes. Penetration testing was performed process involves four phases as shows in Figure 1.

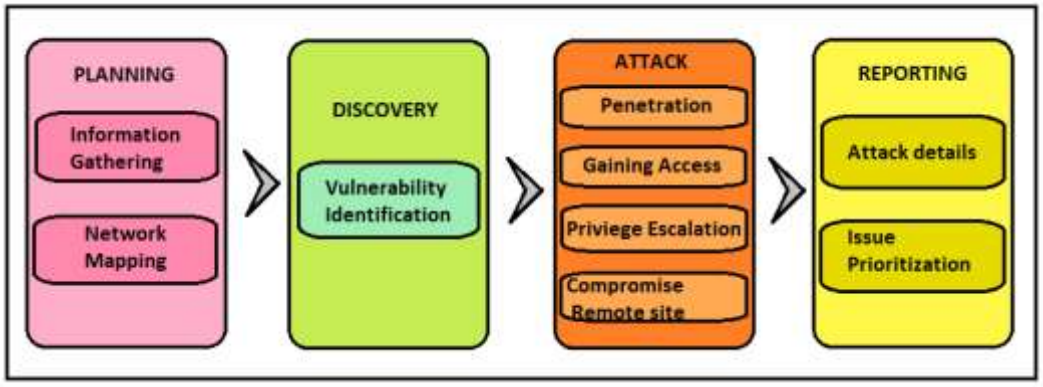

Figure 1: Four phases penetration testing methodology

a) **Planning Phase:** The assignment's scope is defined at the planning phase. Management approvals, paperwork, and agreements such as the NDA (Non-Disclosure Agreement) are signed during this period. Existing security regulations, industry standards, and best practises are all considered by the penetration testing team while preparing a plan for the assignment that are some of the factors that will go into determining the scope of the test. There are types of factor that must be taken into account in order to carry out a well-planned and controlled attack A hacker nowadays has plenty of time to meticulously plan his attack. For a penetration tester, it is a time-limited activity. A penetration tester is obligated by the terms of a legal contract, This outlines the permissible and unacceptable measures a penetration tester must adhere to because they may have a significant impact on the target organization's operations.

b) **Discovery phase:** The actual testing begins during the discovery phase. It's possible to think of it as a data-gathering phase. Vulnerability analysis phase is a part of discovery phase. Following the successful identification of the target systems and the gathering of the required information from the preceding phases. A penetration tester should attempt to find all conceivable flaws in each target system. A penetration test may utilise automated tools to search the target system for known vulnerabilities at this phase. These tools almost always have their own database with the most recent vulnerabilities and their details. Nessus, Shadow security scanner, Retina, ISS Scanner, SARA, and GFILAN guard are just a few examples.

c) **Attack phase:** The third phase in the process is the attack phase. As the name suggests, it is responsible for performing the attacks on the system. The attacks are performed on the vulnerabilities that have been discovered through the discovery phase. The attack phase is completed in a cascaded manner where every successful attack leads to obtaining more privileges and system information. The attack phase is "the heart of any penetration test". This phase is the most interesting as well as the most difficult. This stage can be divided into two parts:

- Penetration: Penetration is a type of attack that tries to break through opposing defences on a regular basis.
- narrow front to throw the defensive system.
- Gaining access: Web application attacks are staged to uncover a target's vulnerabilities. The terms refer to when an attacker gains the access in NETWORK, SYSTEM or APPLICATION.
- Privilege Escalation: There have been times when a successful exploit did not result in access being granted. For example, the penetration tester might gain user-level access to a specific vulnerability. At this stage, an effort should be made to do further investigation on the target system in order to obtain further information that could lead to obtaining administrator power, such as a local vulnerability. The additional privileges gained are leveraged to launch more attacks on other targets. This loop is continued until all the objectives of the attack phase are completed. The attack phase requires constant monitoring to ensure that the system is stable at all times. There is a possibility of an attack being

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

successful and causing serious damage on the system.

- Compromise Remote site: Identifies attacks with evidence. It helps to reduce and control the breach impact. It improves competencies for incident response and detection.

- **Reporting phase:** The reporting phase is the final stage of the whole activity, This stage may occur concurrently with the previous three stages or after the conclusion of the attack stage. Many penetration testers don't pay attention to this stage and rush through all of the submissions. The final report must be written with both management and technical considerations in mind, outlining all findings with appropriate graphs and figures. In order to offer a clear picture of the vulnerability and its implications for the target organization's business. For example, the following items should be included in the report:
- Attack Details: The final report must include the details of the vulnerabilities found, the attacks performed and the analysis of log files.
- Vulnerabilities found, the attacks performed, and the analysis of log files.
- Issue Prioritization: The high risk issues find during testing are reported in detail and are moved to high priority items regarding risk mitigation strategies are concerned. It is essential that the reporting is done with attention to the severity of issues and prioritization.

2.3 Tools for penetration testing

There are a different type of tools and important tools that are used in penetration testing

a) **Nmap:** Nmap is capable of scanning a wide range of protocols as well as the majority of current systems. It is called network mapper. It helps to create network maps and services Nmap analyses the responses after sending specially designed packets to the target host.

b) **Burp suite:** One of the most widely used penetration testing and vulnerability detection tools is the Burp Suite. Its primary purpose is to assess the security of web applications. Proxy-based tools are sometimes known as "Burp." Burp is a tool for testing and evaluating the security of web-based applications.

c) **Metasploit:** Metasploit is one of the penetration testing tools. It helps to Examine operating systems and applications for flaws. The concept of 'exploit' is at the heart of these penetration testing tools. It works on Linux and Microsoft windows.

d) **Nessus:** Nessus is a penetration testing tools and remote security scanner also. It is Typically, a scan of the services offered by a remote machine is performed on a single machine. Nessus is the most widely used vulnerability scanner in the world. Nessus is Scripting and running customized vulnerability checks is possible. Vulnerability checks provide you a lot of control in a way that most other products don't.

e) **Cain and Abel:** Cain and Abel most of the time used for password cracking. It employs techniques such as network sniffing, dictionary attacks, brute-force attacks, and crypt analysis. This is just for Windows-based operating systems.

Table3: Comparative Study of all tools

Tool	Pros	Cons
Nmap	• Nmap is great at finding live hosts on the network. • Nmap is great for teaching new cyber specialist how network reconnaissance works • Nmap is built into every major recon tool on the market, it just when it comes to scanning.	• There could be more built in tools for further vulnerability scanning. • Command line Nmap should store recent scans automatically. • More detail in the help menu for what some of the triggers actually do.
Burp Suite	• The ease of installation for both community and paid version. • The simple interface makes it the most user friendly tools for security testing. • Availability across all platforms helps a lot in switching environment.	• Burp suite can try to add graphic representation to make it even more helpful for users. • There should be an option to recover a project which is not currently saved on disk. • There should be an option which enables the tester to change the response in Repeater to see what it results in.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 9 | September 2021 - Peer Reviewed

Metasploit	• Growing community of users. • Growing documentation. • Excellent tool to identify and exploit vulnerability.	• Difficult to learn. • Lesser GUI based support. • Requires deep knowledge for exploit development.
Nessus	• Free for non-commercial use. • Good for security Audits. • Scanning multiple hosts on the same scan. • Operates on multiple software. •	• Hard to configure for beginners. • Limited support for Ubuntu, Fedora core, FreeBSD, Debian. • The free non-commercial license is limited to up to 16 IP addresses that must be Within the same household. • Required strong knowledge.
Cain and Abe	• Pros of Cain: Dominance and leadership Personal wisdom and denial of hurting facts • Pros of Abel: Patience and long suffering Humility and goodness	• Cons of Cain: Judgement and punishment Mistrust and low opinion • • Cons of Abel: Falling prey to other bad people Failure for self-defence

3. FUTURE SCOPE

The capacity to protect industries from various cyber-attacks is a major driving reason for penetration testing growth, as an increase in the incidence of cyber-attacks can increase the vulnerability of key data maintained by organizations and have a negative impact on revenue.

The current work could be expanded in the future along the following lines::

- Performing the penetration testing and vulnerability assessment to the rest of the university network and more number of virtual machines.
- Developing new techniques or algorithm to speed up and Integration of used tools into one tool to ease of task of duties involving penetration testing and vulnerability assessments.
- Including additional parts of penetration testing and vulnerability assessment, such as traffic analysis and hardware configuration, in some areas of penetration testing and vulnerability assessment also.

CONCLUSION

The present paper reviewed studies in the field of penetration testing especially web penetration test. Manual penetration test is not effective in terms of time and money, so its automatic version is considered. For performing the automatic web penetration test web scanners are used. they first crawl the target, then attack to the result of the previous phase and finally report vulnerability in the target.

In this paper, we examined research in the field of web penetration test in three categories: articles that compared and analyzed available scanners, articles that proposed a new method or tool for penetration test and articles that proposed a test environment to test different tools. According to papers that analyzed various scanners, the Acunetix Web Vulnerability Scanner and IBM Rational AppScan scanners and the SQL injection and XSS vulnerabilities were considered more than others. We also reviewed 10 studies that proposed a new tool or method for penetration test, some of which were based on the dynamic analysis, some on the static analysis and some on a combination of the two. To evaluate any method or tool in the field of penetration test, we require test environments. Four test environments were introduced in the final section. The problems in existing scanners include the lack of support of attacks like stored sql and stored XSS that need to several steps to complete the attack, the lack of support of new technologies and vulnerabilities related to application logic flows. It is hoped that future work will consider these items.

REFERENCES

1. *Lam K, LeBlanc D, Smith BI (2004) Assessing network security. Redmond, wash. MicrosoftPress, Washington*
2. *X.Y.B.-T.B.C.M.J. "AN OVERVIEW OF PENETRATION TESTING," International*

Journal of Network Security & Its Applications (IJNSA), vol.3, no.6, 2011. Aileen G. Bacudio,

3. *"Ethical Hacking and Penetration Testing Strategies," International Journal of Emerging Technology in Computer Science and Electronics (IJETCSE), vol.11, no.2, pp. ISSN 0976-1353, 2014.*
4. *"Vulnerability Assessment and Penetration Testing," International Journal of Engineering Trends and Technology-, vol.4, no.3, 2014. K,K.K. Amkita Gupta,*
5. *"Seven Pharse Penetration Testing Model," International Journal of Computer Applications, vol.59, no.5, p. ISSN:0975-8887, 2012. P. Ami and A.*
6. *McGraw, G. Software Security: Building Security In, Adison Wesley Professional, volume 4, issue 7, September 15, 2006. The Canadian Institute of Chaetered Accountants*
7. *Arkin.B., Stender, S., and McGraw, G. "Software Penetration Testing," IEEE Security & Privacy volume3, issue: I, jan-feb. 2005, pp 84-87.*
8. *Zaher Al Shebli, H. and Beheshti, b. (2018). A Study on Penetration Testing Process and Tools. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT),17842208. https://doi.org/10.1109/LISAT.2018.8378035*
9. *MainkaC, SomorovskyJ, SchwenkJ (2012) Penetration testing tool for web services security. In: SERVICES '12 Proceedings of the 2012 IEEE Eighth World Congress on services. IEEE. Pp 163-170*
10. *Nidhi Vora, Chandresh Parekh " Vulnerability Assessment and Penetration Testing in Web Application and Its Prevention" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, volume2, issue 6, 2017.*
11. *Jai Narayan Goela, BM Mehtreb "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology" Peer-review under responsibility of organizing committee of the 3rd International Confrence on Recent Trends in computing 2015 (ICRTC-2015) Doi:10. 1016/j.procs.2015.07.458.*
12. *Dixitkumar .V. Prajapati, Deepak Upadhyay, "Cyber Defence: A Hybrid Approach for Information Gathering and Vulnerability Assessment of Web Application (Cyberdrone)," International Journal of Computer Sciences and Engineering, Vol.7, Issue.5, pp.65-72, 2019.*