PENETRATION ANALYSIS ON INTERNET DEVICES USING PENTESTING METHOD AND SECURITY MECHANISM

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

PARAMPREET KAUR

Registration number: 11206721

Supervisor

Mr. ANKUR SODHI

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

April, 2017

PAC form

ABSTRACT

The penetration testing is the technique that detects the penetration value from the network. The rank-to-learn algorithm is applied which gave rank to each feature of the network to check penetration value. The back propagation algorithm is applied which increase the penetration value of the rank-to-learn algorithm. The proposed algorithm is implemented in MATLAB and it is been analyzed that execution time is reduced, penetration value is reduced.

Penetration testing is a custom or method to find the vulnerability of a system and exploit it. The main mission of pen testing is to provide a secure data. This report figure out the cause of vulnerability, types of pen testing and procedure of handling penetration method. This work also focus on the security mechanism of the system. Pentesting method is very helpful for the organization to store the data securely. Pentesting basically find the weakness of the system and report to the system administrator then the reports are used by the administrator to improve the security standard of the system for future purpose.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled "PENETRATION ANALYSIS ON INTERNET DEVICES USING PENTESTING METHOD AND SECURITY MECHANISM" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Ankur Sodhi. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Parampreet Kaur

11206721

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**PENETRATION ANALYSIS ON INTERNET DEVICES USING PENTESTING METHOD AND SECURITY MECHANISM"**, submitted by **Parampreet Kaur** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Mr. Ankur Sodhi

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

Gratitude cannot be seen or expressed. It can be felt in heart and is beyond description. Often, words are inadequate to serve as a model of expression of one's feeling, especially the sense of indebtedness and gratitude to all those who help us in our duty. It is of immense pleasure and profound privilege to express our gratitude and indebtedness along with sincere thanks to my mentor **Mr. Ankur Sodhi** for providing us the guidance to work for the dissertation on "**Penetration Analysis on internet Devices Using Pen testing Method And Security Mechanism".**

We want to formally acknowledge our sincere gratitude to all those who assisted and guided us in completing this dissertation report.

Parampreet Kaur (11206721)

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Penetration Testing

Network pentesting is a method for agencies and different organizations to find away approximately vulnerabilities of their network safety before hackers use them to break in. One of a kind forms of network pentesting exams are categorized and the simple way to take a look at is printed. Different equipment and strategies which might be used in every phase of the check are introduced. The purpose is to provide a trendy outline of the strategies hired in community pentesting trying out in addition to identifying the destiny developments and in addition research guidelines in pentesting testing and community protection.

Pentesting is path toward endeavoring to get to assets without learning of usernames, passwords and other typical methods for get to. On the off chance that the emphasis is on computer resources, then examples of an effective penetration would get confidential documents, pricelists, databases and other protected information. The primary concern that isolates a penetration tester from an attacker is permission. The penetration tester will have permission from the proprietor of the computing resources that are being tested and will be responsible to give a report. The goal of a pentesting is to increase the security of the computing resources being tested. By and large, a penetration tester will be given user-level access and in those cases, the goal is elevate the status of the account or user different means to access additional information that a user of that level ought not have admittance to. Some penetration testers are contracted to discover one hole, yet as a rule, they are expected to continue looking past the first hole so that additional vulnerabilities can be identified and fixed. It is imperative for the pen-tester to keep fundamental notes about how the tests were done as such that the results can be verified thus that any issues that were uncovered can be resolved. Understand that it is far-fetched that a pen-tester will discover all the security issues. As an example, if a penetration test was done yesterday, the organization may pass the test. In any case, today is Microsoft's "patch Tuesday" and now there's a brand new

vulnerability in some Exchange mail servers that were already viewed as secure, and next month it will be something else. Keeping up a secure network requires constant vigilance.

Pentesting uses are:

1. Decide whenever and by what method pernicious client increase unapproved access for resources which influence crucial safety about framework, records, potentially information.

2. Approve that pertinent authority, for example, capacity, helplessness administration, strategy, also division, necessary for PCI DSS set up.

Three sorts of pentesting: Black, White, also Grey box.

In the first one, customer gives no data preceding begin of testing. In the second one, element may give pentester full and finish points of interest of system also of applications. For third one appraisals, element give halfway points of interest of objective frameworks. PCI DSS pentesting are commonly executed either white or grey box evaluations. Mentioned sorts of appraisals gain extra precise outcomes also give far reaching trial for security stance of earth then a unadulterated discovery appraisal. Discovery appraisals offer next to no in the method for incentive for PCI DSS entrance tests, since the substance gives no subtle elements of the objective frameworks preceding the begin of the test, the test may require additional time, cash, and assets to perform [20].

Pentesting is method of approving the impact of exceptional well being vulnerabilities or erroneous systems. It is an authorized attempt to take advantage of device vulnerabilities consisting of operating machine, protocol stacks, applications, misconfigurations or even volatile cease person behaviour and so on. It uncovers the limit results of a group being bargained or hacked by methods for a real aggressor. This method includes an intensive energetic search of barrier associated functions of target gadget, follow by way of an endeavor to interrupt system via rupturing those agreement functions. These exams can be led utilizing exclusive hardware. Security vulnerabilities knowledge effectively exploited thru alike checking out enables producing file that focus all of the uncertain ranges that need interest of gadget managers.

The crucial thing is longings to be comprehended is that one might be effective in locating masses of vulnerabilities , however except these effects evaluate and check could not either upload part of enormous amount to enterprise part of corporation.

1.2 Four States of Pentesting:

1. Pre-engagement collaborations

Pre-engagement collaborations is making plans segment, during which the extension for the undertaking is depicted. Approvals of Management, files and NDA (Non Disclosure Agreement), and many others. are registered. The pentesting crew develop particular approach for venture. Actual safety regulations, enterprise code, pleasant rules, and so on act as input to define the scope of test. The indicated step commonly contains sports which can be finished previous to graduation penetration check. There are diverse aspect which are consider for running a well mannered plan assault . Penetration tester has so many boundaries while test finishing, for this reason right success penetration check is required. Some constraints are:

• Time: Hacker has spacious time for implementation his assault. He sticks to planning.. Components like companies working hours taken into consideration.

• Legitimate Limitations: Pentester is certain via prison settlement, who provides perfect also suitable steps a penetration tester should observe usually because this may want to includes results at the commercial enterprise of enterprise. Some other boundaries that organization forcefully stick on Pentester that include enterprise effect, like, records, etc. The mentioned elements are necessary taken into consideration all through this stage.

2. Skill Meeting

Skill meeting collects segment, that pentester knows the target, inclusive of the way it behaves, the way it operates, and how it in the long run may harmed. Collected facts grant benefical perception toward safety discipline. Meanwhile meeting amassing, try earns increased viable knowledge vacant business goal enterprise the use of diverse way, both technical in addition to nor scientific .

Later efficiently describing accessible gate, offerings in the back of them must noticed. Usually the suggestion is pentester affirm real call along with bussiness model strolling at goal device also hidden OS previous inclusive of like inside last document. It will assist by finding along with putting off different untrue close up located after.

Pentester should use these steps with feasibility also innovative sufficient by finding numerous way out along with discovering each feasible issue which can result in relevant data leakage approximately the target company inside the shortest time viable.

3. Error Testing

In error evaluation, statistics are gained by previous steps that are combined also using it for discovering the feasible error inside goal device. A penetester can also have automatic devices for checking goals. Equipment normally contains their own records to store error along with its specification. Success penetester would continually preserve their knowledge up to date along ultra-modern error using becoming a member of security related mailing-lists, protection blogs, advisories, and so forth.

4. Displaying

Displaying represents standout amongst energizing components include in pentesting. Unanticipated defensive part may set up objective which keeps specific endeavor to working. In any case, untill activating powerlessness, pentester ought to any rate turn out to be certain framework. Constantly prudent is lot of finding objective, along afterward dispatch all around investigated abuses which probably going to succeed**.** Amid during stage an pentester attempt for discover abuses, different errors found for past stage**.**

5. Before Displaying

Essential element of pentesting take a look at. Post exploitation objectives particular structures, identifies essential infrastructure, and objectives statistics of organization amount maximum along with relaxation. Attempt must designed for future testing at goal device for profit greater knowledge should result in gaining benefit in market.

6. Final Step

A long way maximum vital including pentesting components check. It is communicating channel that tells us way the testing have been carried out, and, most crucial, how the employer must restore the vulnerabilities discovered for the duration of the pentesting. Along with appearing pentesting check, person have to response according to hacker, businesses hardly ever seen. Statistics gained in the course of a take a look at is crucial to the achievement of the employer's records protection program and in preventing destiny assaults.

The findings must be compiled and mentioned in this kind of way company could increase recognition, remedial troubles found, also enhance inclusive safety comparatively focusing on some other error. Document need to specific also exact . Nothings have remain for patron's creativeness. Fine, unique documents constantly always indicates capability.

For example the necessary things that the document must include:

• Managerial brief

• Precise Decisions

•Prospect stage:- error discovered

• Market Effect

• Suggestions

• Outcome

Chapter 2

LITERATURE REVIEW

Matthew Denis, et.al (2016) proposed on this paper that penetration trying out secures networks, also focus on safety concerns. They look into specific parts of penetration testing such as gear, assault techniques, and defense strategies. More in particular, we carried out extraordinary penetration exams utilizing a personal networks, gadgets, and virtualized systems and equipment. The attacks we accomplished protected: mobile pentesting, Preserved Wi-Fi, having access to computer receiver, etc. Penetration gear have been getting a notable deal of attention, considering that there aren't any barriers for their route of producing. Open source tools can be changed agreeing singular desires. Envision of penetesting a device for unauthorized access to change maintenance for climate arrangements, or possibly exchange the time, or even worst to dynamic atomic sword. Current days, making use of those tools, we are able to hack medical gadgets, or maybe automobiles. This paper detailed essential penetration trying out assaults and talks about potential mitigation processes. The consequences are then abridged and pointed out. The paper likewise laid out the detailed steps and techniques while carrying out these attacks [22].

Jai Narayan Goel, et.al (2016) proposed in this paper that vulnerability estimation and is essential motion to upgrade networks protection of systems. Yet, it is far high priced system. Superior VAPT equipment were valuable. Indeed, alike top class VAPT equipment are not ready to present a hundred % accuracy to discover vulnerability. Notwithstanding , simple VAPT tool cannot discover full error. Hence we require version which could discover sort error, grant just about one hundred % accuracy and don't fee extra. To accomplish this purpose we formed Ensemble path of VAPT gear. Our way joins numerous VAPT gear (top rate) also applies more balloting and complete precedence. Our method offers improved efficiency along with increase utility. Our technique offers amount efficient way to error testing and pentesting checking out. Later on they created software which put in force that way referred to as 'VEnsemble 1.0'. We get likewise supplied applied software along outcomes.In Future VEnsemble can changed into completely computerized form with the intention which is able to hold consequences immediately from yield regardingVAPT gear.

Finally this solution is extraordinarily efficient in phrases of value and sources. This may be extraordinarily powerful solution of costly and less exact VAPT system [23].

Herny Ramadhani Husny Hamid, et.al (2015) proposed on this paper that the simple citadel of safety toward shield a community along firewall. To have intelligence in security, previous disclosure should support from undergrad stage to facilitate the evolution of intelligence and getting to know method. Current students who're considering in security area seldom have own opportunity to exercising arms-on motion in magnificence because of time necessity and absence of framework in an academic corporation. To assist the activity of giving disclosure some of the students conquer the preceding complication, an technique to build up a convenient pentesting along firewall composition toolkit has been suggested as a studying help for the understudies to carry out pastime on accomplishing pentesting along compose firewall as novices. From the proposed toolkit, pupils are geared up to run simple pentesting checking out, network tracking, port checking, firewall composition, web and penetrate everywhere and at something time. Carrying these proposed toolkit, training and gaining knowledge of system will be notably less difficult, green and efficient in comparision to standard practice of coaching [24].

A. K. Pathak, et.al (2015) Proposed in this paper that the degree of strength being produced by means of wind mills is growing persistently and wind electricity penetration is frequently finishing up it appears that evidently extra little by little. Because of enormous varieties in wind generation, reactive power streams on transmission lines and voltage are most important variables. This paper provides the modeling and reproduction of Static Var Compensator (SVC) and reactive electricity manipulate. In the first step, modeling of SVC finished. In the second step, modeling of SVC is configured in strength gadget to break down its conduct for reactive energy manage alongside effect on voltage stage in 659 transport structures of Rajasthan Grid, comprising of different voltage degree with excessive wind strength penetration in the power system. All analysis is anchored with load movement evaluation for SVC awareness, with the aid of utilizing Mi.- Power system analysis software program. The wind power neither is available in step neither one of the reductions is in step, in actual area situation it is truly unpredictable. Wind technology is associated as bad load for analysis cause. Additionally place insightful wind strength technology is distinctive. The better SVC modeling wishes to drastically consider these affects additionally and there may be a awesome deal of scope for future work if effects are acquired with thyrister managed reactor

and capacitor and compared with constant capacitor SVC for comparative circumstance. Results of checks led at the version device in special possible subject situations [25].

Marri Rami Reddy, Dr. PrashanthYalla, (2016) proposed in this paper that each one the wellness vulnerabilities which can be gift in the machine must be uncovered with penetration checking out. Vulnerabilities are brought about because of Designing and evolution flaws, Human mistakes, low device composition. We centered on exclusive styles of pentesting checking out practices, for example, Social Engineering, Application Security Testing and Physical Pentesting. We concentrated on one of a kind tools involved at distinct instances at exceptional techniques, specs, necessities, arranging and checking for fruitful penetration checking out practicing automatic equipment, standard processes and auto-standard procedures tools. The mathematical and algorithmic form is tested and validated along the undertaking and graphs, at lengthy last layout and practice of pentesting trying out tool is inclined with realistic study and end result. Cyber Security and Code Security are the primary responsibilities in Testing, in which protection is the important assignment in companies global as assaults on code or cyber can cutoff the income and reputation of the commercial enterprise challenge. The most important function of penetration checking out is to recognize and connect the vulnerabilities like malicious code. At lengthy final we closed by improvement of records safety planning and devices which help the Penetration Testing and position of Advanced Pentesting and capacity of characteristic work [26].

Kamran Shaukat, et.al (2016) proposed in this paper that safety is a international trouble. People require their statistics and frameworks relaxed from noxious risks and assaults. A framework need to be secured all around from unlawful penetration. Security best confirmation tests if the utility is defenseless against assaults, if everybody can hack the structure to the utility with no support. It is a method to find out that an statistics framework protects knowledge and maintains up efficiency as suggested. While pentesting trying out is the technique that organize accumulating information approximately the goal earlier than the test, spotting feasible section center, determine to melt up and describing lower back the disclosures. We have overlook special structures which may be protected at testing level thru the pentesting trying out way and planned an front testing process to relaxed structure like databases, networks, internet applications and Android. Huge trying out issues clean confirmation of trouble and provide a planning phase of registering plan. The purpose of meeting of pentesting trying out is excessive fact weakness and there is no false high quality about it. In one section; ruin the device thru hacking and in 2d part; make device extra

comfortable by utilising the results of first element; and it is all manifest inside the take a look at. In future we can carry out more paintings on this domain with the aid of performing this methodology at the structures given in this paper [27].

Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar, (2016) proposed on this paper that during most current 1 / 4 century, of web programs, net hacking activities have misrepresented quick. Organizations confronting incredibly critical demanding situations in securing their internet packages from increasing cyber risks, as alternate off with the safety problems don't appear like acceptable. Vulnerability estimation and Pentesting structures assist them to head watching out security way out. These security way out should likewise be exploit by attackers to release assaults on specialized property. In this manner it's miles essential discover these vulnerabilities and installation security strips. VAPT allows business enterprise to decide whether or not their security preparations are functioning as it should be. This paper intends to explain define and special strategies applied as part of vulnerability estimation and pentesting. Additionally makes a speciality of making cyber protection consciousness and its significance at distinct level of an agency for reception of mandatory updated security measures by means of the agency to remain covered from exceptional cyber-attacks. To make VAPT consequences important it requisite estimate and clarify vulnerabilities with CVE numbers which may be purchased from enterprise trendy references like countrywide vulnerability database (NVD), ordinary vulnerability scoring system (CVSS), open source vulnerability database (OSVDB) and so forth. Likewise those outcomes can deliver potential remediation tips to identified vulnerabilities [28].

Siripong Roongruangsuwan et al (2010), In their research they proposes two different valuable method for take a look at case prioritization. The first approach is advanced to solve the trouble of many check cases having the equal weight values. The 2nd technique is designed to prioritize multiple suites successfully. These two techniques decrease a prioritization time. This paper specially offers interest to check case prioritization strategies handiest. This paper describes four types of take a look at case prioritization techniques, which are: (a) purchaser requirement-based totally strategies

(b) coverage-based strategies

(c) Price effective-primarily based techniques

(d) Chronographic history-based techniques

First, the client requirement-based strategies are methods which prioritize check cases primarily based on requirement specifications. Second, the insurance primarily based techniques are white-box testing strategies. They evaluate check program behaviour against the supply code. In contrasts with useful black-box checking out, which compares take a look at software behaviour against a requirements specification. Third, the cost powerful-based totally techniques which prioritize take a look at cases based on fee elements, like fee of evaluation and fee of prioritization. Last, the chronographic history-based totally techniques which prioritize test cases base on check execution records elements. From this paper we additionally study that there are numerous difficulties and gaps within the test case prioritization. [29]

Hyunsook Do et al (2010), This paper display the effect of time constraint on take a look at case prioritization. Time constraints turn out to be a cause to advanced prioritization strategies and stepped forward protection and testing methods. Time constraints that can be carried out on testing by using various software development processes can strongly affect the behaviour of prioritization strategies. [30]

Alien G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, "Overview of Penetration Testing", 2011 in this paper they explained that security is the one of the superior topic of information systems. The growing use of computers through internet, the growing compliance of systems has made security a bigger question. Penetration testing is one of the security mechanisms to improve the security of the system. It is used to check the security of the application. Pen testing can used to find vulnerability in many internet devices like mobile phones, web application, servers, Computers etc. Vulnerability can be due to design, software bugs errors etc. It identify the Weak areas where hacker can attack, protects the original data. The Penetration process consists of 3 phases that are test preparation, test and test analysis. Under the test phase we have information gathering, vulnerability analysis and vulnerability exploit. The penetration testing is of different types like network pen testing, web application pen testing etc. The benefits of the pen testing are providing protection from damage, update the system in proper manner. Penetration testing can be black, white or gray box depending upon the amount of information with the user [31].

Konstantin us Xynos, Iain Sutherland, "Penetration Testing and Vulnerability Assessments: - A Professional Approach", 2010 in this paper, they explain that in today time, the attacks to the computer systems are increasing day by day. There is "zero-day" is a vulnerability hole that the vendor does not know. This hole is used by hackers as a good opportunity to attack before vendor knows about it and try to fix it. It includes malware, spyware or access of unwanted user to information. To protect from these types of attack one method is to appoint the pen tester team to find vulnerability which is present in the network and provide best way to deal with them. Pen tester motive is to improve security. There are 3 recognized certification are CHECK, TIGER and CREST scheme [32].

CHECK: **-** Any organization who wants to perform a penetration test of systems, they first need to become a check service provider. There is an assumption that anyone who performs this scheme holds security clearances of UK. It is available only for the government organizations.

CREST: **-** It is Council of Registered Ethical Security Testers. It is available for both private and public sector. There is a proper guidance's provided to members on standards, code of practice, methodologies and further recommendation.

TIGER: - It consists number of levels from Associate membership till the senior tester qualification. It is multi-tiered candidate system. Candidate can award TIGER scheme without having clearances of UK security.

Network Penetration Testing and Research Brandon F. Murphy, 2013in this paper ,they explained that network security is one of the growing field and also one of the concerning field. There are many issues related to the research process one of them is system updates. We use many tools for pen testing like Nmap, Nessus, and Reaver etc[33].

Chow, "Ethical Hacking and Penetration Testing ACC626:- IT Research Paper", 2011 in this paper , they explained that ethical hacking and pen testing is preventive measures having legitimate tools to identify, exploit company's weakness about security. Penetration Testing Techniques are:-

- Web Application Software: - In this we use of firewalls, cookies, strength of passwords, encryption.

- Denial of service: - The system can deny service from authorized user due to the vulnerability or become totally not available due to high traffic.

- Wireless Network: - Pen testers identify error in design, operation and implementation of wireless network of a company.

- Google Hacking:- One of technique used to get personal, sensitive information taking advantage as it is search engine.

Combination of Pen testing Strategies and techniques are used to obtain effective level of security in any organization. Ethical Hacking and Penetration Testing are effective ways to close gaps of security, deficiencies before any hacker exploit them [34].

Len Klein man, "Vulnerability Management and Research Penetration Testing Overview", 2013 in this paper , they explained what vulnerability management, its role and responsibilities. It also explains what is the pen tester is what are the different types of hackers there are like black the cracker one, white which is known as the ethical hacker and the last type is the grey who disclose the all activities. It also defines the steps which are helpful to develop ones capability. Penetration testing in terms of vulnerability management is explaining in four phases like test phase, reporting phase and also structure of a pen test. At last it defines the challenges, benefits and the consequences to the challenges in pentesting[35].

Parag Pravin Shimpi, Sangeeta Nagpure, "Penetration Testing:- An Ethical way of Hacking", 2015 in this paper ,they explained the concept of ethical hacking and penetration testing. It also introduces the four step methodology consist basics of maintaining access, reconnaissance, exploitation and also the post exploitation. It also explains the examples in the virtual environment. It helps to understand the information about the ip configuration and provides us with some virtual examples for practice [36].

Gordon Fraser, "Tunneling, Pivoting and Web Application Penetration Testing", 2015 in this paper, they explained the concept of pivoting. When we are conducting the pen testing of a web application there are some cases came where you pivot to some other system to gained access to continue the testing. The five common use pivot channels are SSH local and dynamic port forwarding, Net cat relays, Ncat HTTP proxy and Meterpreter sessions. Pivoting is one of the important techniques in the pen testing and it allows to bridge networks over intermediate system. Different tools used for pivoting are the Nmap, W3af etc[37].

Maxim Catanoi, "Penetration Testing: Alternative to Password Cracking", 2015 in this paper , they explained that the penetration is the art of finding the ways to break the networks and servers so that they can assess at their actual security level. The pen tester always think something different mean something out of box so that the pen testing is performed at the comprehensive level. This paper defines the ways by which the pen tester can get the password of the user. They can use the obtained credentials to obtain access to the other system inside and outside of that organization. It defines the ways to find the complexity of the passwords[38].

Matt Koch, "Web Application File Upload Vulnerabilities", 2015 in this paper, they explained that the type of vulnerabilities find when we upload the file on any web application. They explain that the vulnerabilities associated to the file upload are highly destructive. This paper also explains the ways to discover and exploit the vulnerabilities. File upload vulnerabilities reveal the unknown vector as way for the cross-site scripting and SQL injection vulnerabilities. It tells us that it is important to include the file uploaded vulnerabilities in the pen testing [39].

Andrew Andrasik, "In but not Out: Protecting Confidentiality during Penetration Testing", 2016 in this paper , they explained the techniques, procedures and tactics to implement the ethical hacking to finish their testing within the limited scope reducing the stress related to the confidentiality which helps in protecting data from the unauthorized user [40].

Jianming Zhao, Wenli Shang, Ming Wan, Peng Zeng, (2015) proposed on this paper that the utility to determine the community and machine safety in any key fields, pentesting checking out estimate strategies had been advancing right into a widely known studies factor. In any case, the automation diploma of penetration checking out is at a decrease degree, and severa parameters of security practice technique is questionable. For mentioned two troubles above, we make use of rule timber method to accomplish the automation method of pentesting, and each chain of rule timber stores a entire the assault method. By using the end result of pentesting checking out, we advocate the safety technique to meet the NIST tips, and it may make a few questionable parameters of security practice clear. With the steady extension of rule timber, the proposed method can enhance the capability and effeciency of security practices. By constructing experimental information, we test and look at our method of pentesting check safety practice. Also, those tested the usefulness of this paper technique [41].

Suyash Jadhav, Tae Oh, Young Ho Kim, Joeng Nyeo Kim, (2015) proposed the mobile tool assessment and testing platform to assess the mobile malware. Utilizing the platform, the creators have created some publications in mobile tool protection. One of the vital necessities is to give college students a safe surroundings for malware tetsing. Different functions incorporate tool better lab environment, log series and correct help. Java based client-server application have been invented to serve those needs. Additionally a structure to carry out mobile malware analysis and cellular pentesting trying out is proposed and carried out underneath this studies paintings. Paper focus on breaking down needs for such coursework to do mobile malware evaluation and cell utility pentesting. Paper moreover offers information for the gear create and structure practice to effectively train. Advanced Mobile Device Security route and perform wise lab sports. Likewise the practiced mobile pentesting trying out framework for appearing mobile software pentesting lab physical games offers greater bendy and precise inspecting capabilities to the students [42].

Surya Michrandi Nasution, Yudha Purwanto, Agus Virgono, M. Rifqi Y. Tambunan, (2015) proposed in this paper that keylogger captures all the word due to its dangerous nature that are displaying in console. Two types of keylogger, programming also equipment key logger. Anything but difficult for correction on the grounds that the two already recorded error. This is is extensive measure of antivirus application which identify programming also equipment keylogger, it is effectively checked whether any peculiar element appended with user PC. Kleptoware act as answers for equipment keylogger primary issue.One more issue

happens need is have the sum total of what information have catch inside gadget, and should have keylogger firstly. They also talks how to pick up self-governingly with customer server plan area. Exhibits that information sends in any event have same document measure along cradle which as of now decides first. Consequences related to analysis and examination shows free sender will worked consummately the length of the record measure caught information littler then cradle utilized as a part of the application (for this situation). Each refresh customer's behalf found other side as well. Confinement evaded due to greater measure [43].

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

The penetration checking out is the kind of testing which is implemented at the network to test the security of the network. To practice penetration testing on the network diverse capabilities of the network is taken into consideration and these features are like network kind, encryption type etc. In this work, technique could be implemented which is the greedy approach to stumble on the penetration from the network. In the existing work, technique is applied wherein is the rank to examine primarily based technique to research the community penetration. The rank to analyze approach will rank every characteristic of the network to analyze the penetration of the network. The improvement is needed in the current set of rules to increase penetration detection fee of the algorithm.

3.2 Objectives

1. To propose improvement in the rank-to-learn algorithm to increase penetration detection value of the network.

2. The proposed improvement will be based on Boltzmann learning algorithm to increase penetration value of the network.

3. Implement proposed and existing algorithm , compare in terms of various parameters like execution time, penetration detection value.

3.3 Research Methodology

Learning to rank approach refers to system mastering strategies for training the version in a rating challenge. LTR technique can be used for degree the model performance. LTR is a linear version that is used for optimizing the ranking overall performance at once. LTR model is often used as compare to different models LTR technique may be also evaluate with the prevailing non-linear models. In LTR approach skilled facts may be used. LTR technique cans additionally works on extraordinary facts sets. LTR is useful for plenty programs in statistics retrieval, Natural language processing and information mining. The LTR method obtains a linear model by means of optimizing the rating overall performance immediately. The LTR method can paintings with different models. Count models may be used with the LTR method. Different facts sets can be used in LTR approach for comparing rating of the software program defects. We provide a comprehensive evaluation and contrast of the LTR technique against more algorithms for building SDP fashions for the rating undertaking. The again propagation algorithm is one of the maximum utilized Neural Network algorithms. This approach is used for training the synthetic neural networks and also makes use of the two segment cycle which involves the propagation and weight updates. When an enter network enters the community, it is propagated ahead through the network across each layer until it reaches the output layer. The comparisons are made the usage of the output done in addition to the preferred output. This is accomplished making use of a loss characteristic. For every neuron within the output layer, an error value is calculated. The propagation of the error values is then performed in backward manner which begins from the output. Here, each neuron has its own errors price which additionally shows its contribution to the originally performed output. There are specially 4 steps in which this set of rules may be carried out. The required corrections are to be computed best once the weights of the network are decided on randomly. The lower back propagation set of rules is been carried out which come across the penetration values from the community. The iterations are accomplished and the final new release is that at which most errors are detected. This way rather than changing the hunt engine with an system mastering version, we are extending the manner with an additional step. After the query is issued to the index, the great outcomes from that question are surpassed into the version.

Proposed Algorithm

Improved learning to rank algorithm is

```
t := 0;

int population P (t)
evaluate P (t);
     Network  ConstructNetworkLayers()
      InitializeWeights(Network, testcases)
     For ( i=0;i=testcases;i++)
          SelectInputPattern(Inputfaultvalues)
          ForwardPropagate(p)
         BackwardPropagateError(P)
         UpdateWeights(P )
     End
     Return (P)

           while not done do

               t := t + 1;

     P' := test case P (t);

     recombine P' (t);

     mutate P' (t);

     evaluate P' (t);

     P := survive P,P' (t);

end
```

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Tool Description

The matlab is the device that is used to carry out mathematical complicated computations. In this MATLAB simplified C is used because the programming language. The MATLAB has diverse in-built toolboxes and these toolboxes are mathematical toolbox, drag and drop based totally GUI, Image processing, Neural networks and so forth. The MATLAB is usually used to put in force algorithms, plotting graphs and design user interfaces. The MATLAB has excessive images due to which it's miles used to simulate networks. The MATLAB has numerous variations with the aid of modern MATLAB model is 2015. The MATLAB system factors inside the form of MATRIXs and numerous different languages like JAVA, PYTHON and FORTAN are utilized in MATLAB. The MATLAB default interface has following parts

- **Command Window:-** The Command Window is the first importance part of MATLAB which is used to show output of already saved code and to execute MATLAB codes temporarily.
- **WorkSpace** :- The workspace is the second part of MATLAB which is used to show allocation and deallocation of MATLAB variables. The workspace is divided into three parts. The first part is MATLAB variable,variable type and third part is variable value .
- **Command History** :- The command history is the 0.33 part of MATLAB in which MATLAB commands are shown that are carried out formerly.
- **Current Folder Path** :- The current Folder course shows that direction of the folder in which MATLAB codes are stored.

Properties of MATLAB

- It additionally affords an interactive surroundings for iterative exploration, design and problem fixing.
- It affords massive library of mathematical features for linear algebra, facts, Fourier evaluation, filtering, optimization, numerical integration and fixing everyday differential equations.
- It offers integrated snap shots for anticipating information .
- MATLAB's programming interface offers improvement gear for enhancing code pleasant maintainability and enhancing overall work.
- It offers gear for constructing programs with custom graphical interfaces.
- It gives capabilities for integrating MATLAB primarily based algorithms with external programs and languages which include C, Java, .NET and Microsoft Excel.
- It is a high-level language for numerical computation and alertness improvement.

Uses of MATLAB

MATLAB is widely used as a computational device in technological know-how and engineering encompassing the fields of physics, chemistry, math and all engineering streams. It is utilized in a number of programs consisting of :-

- Image and Video Processing
- Control Systems
- Test and Measurement
- Computational Finance
- Computational Biology
- Signal Processing and Communications

4.2 Comparision with Existing Technique

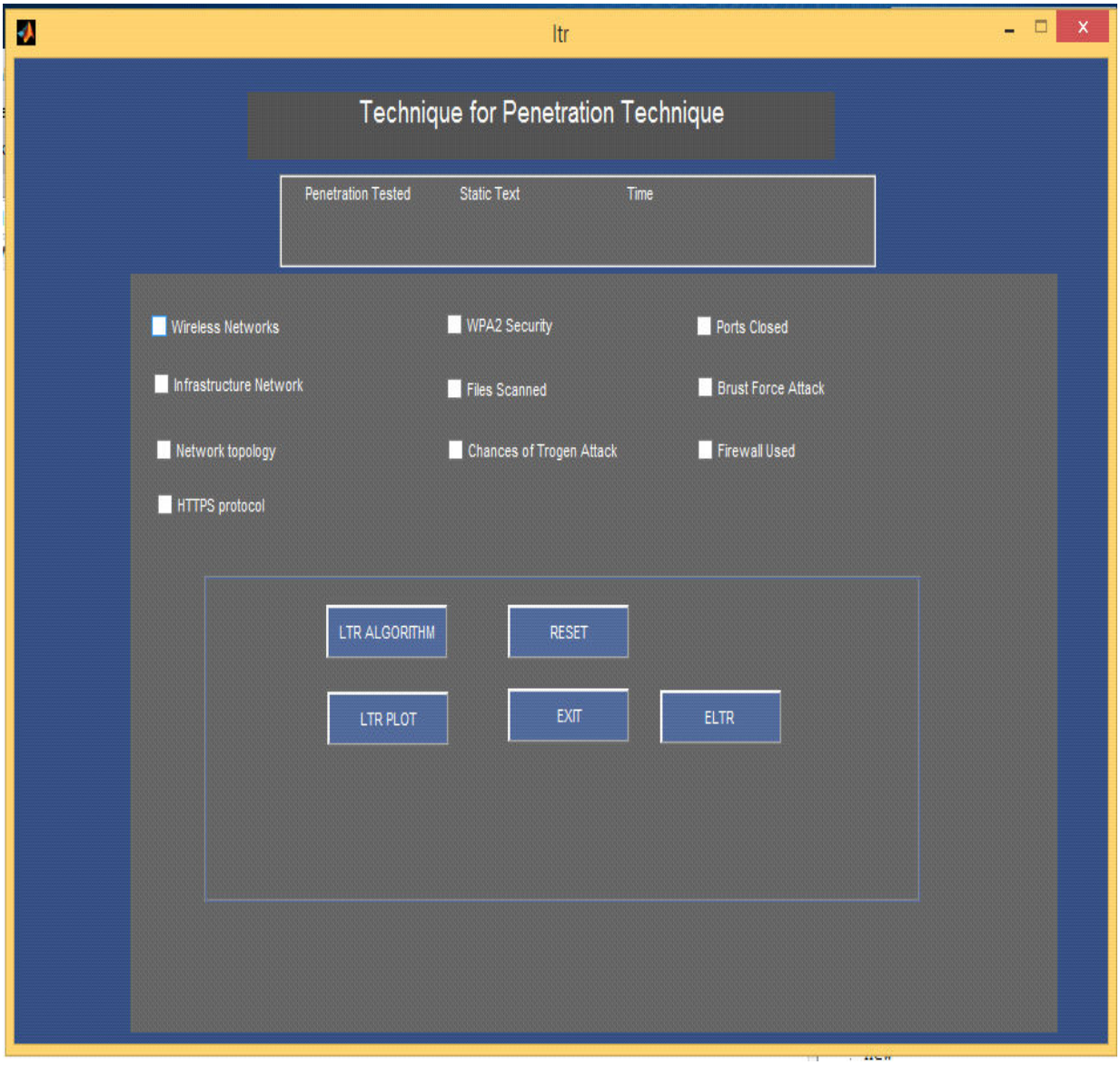

Figure 4.1 Default Interface

As shown inside the Figure 4.1, the interface is designed in which numerous network options are shown that are used for penetration testing

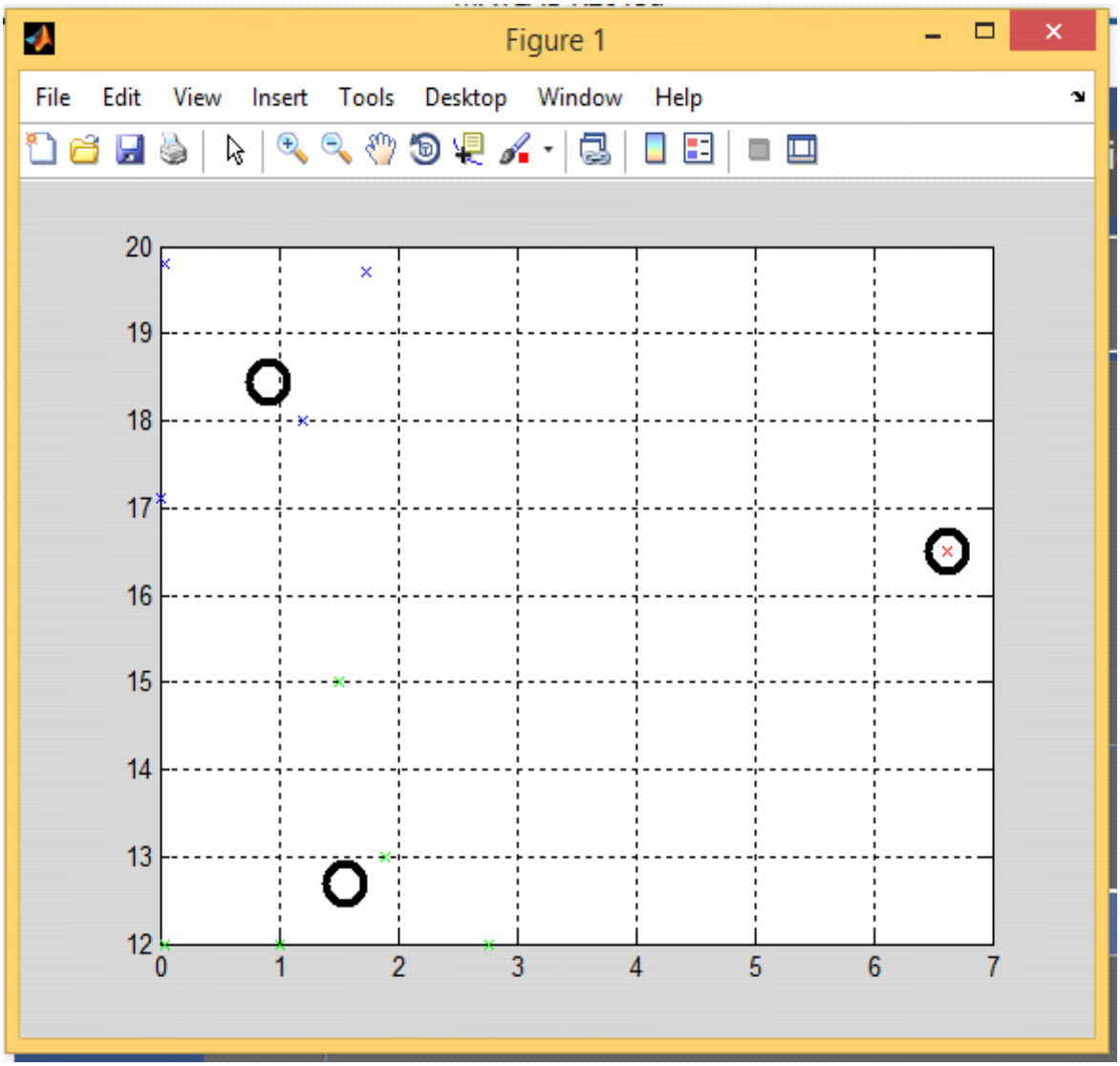

Figure 4.2 Selection of best value

As shown in the figure 4.2, best value is selected from multiple values which are further used to create the final outcomes of the penetration testing

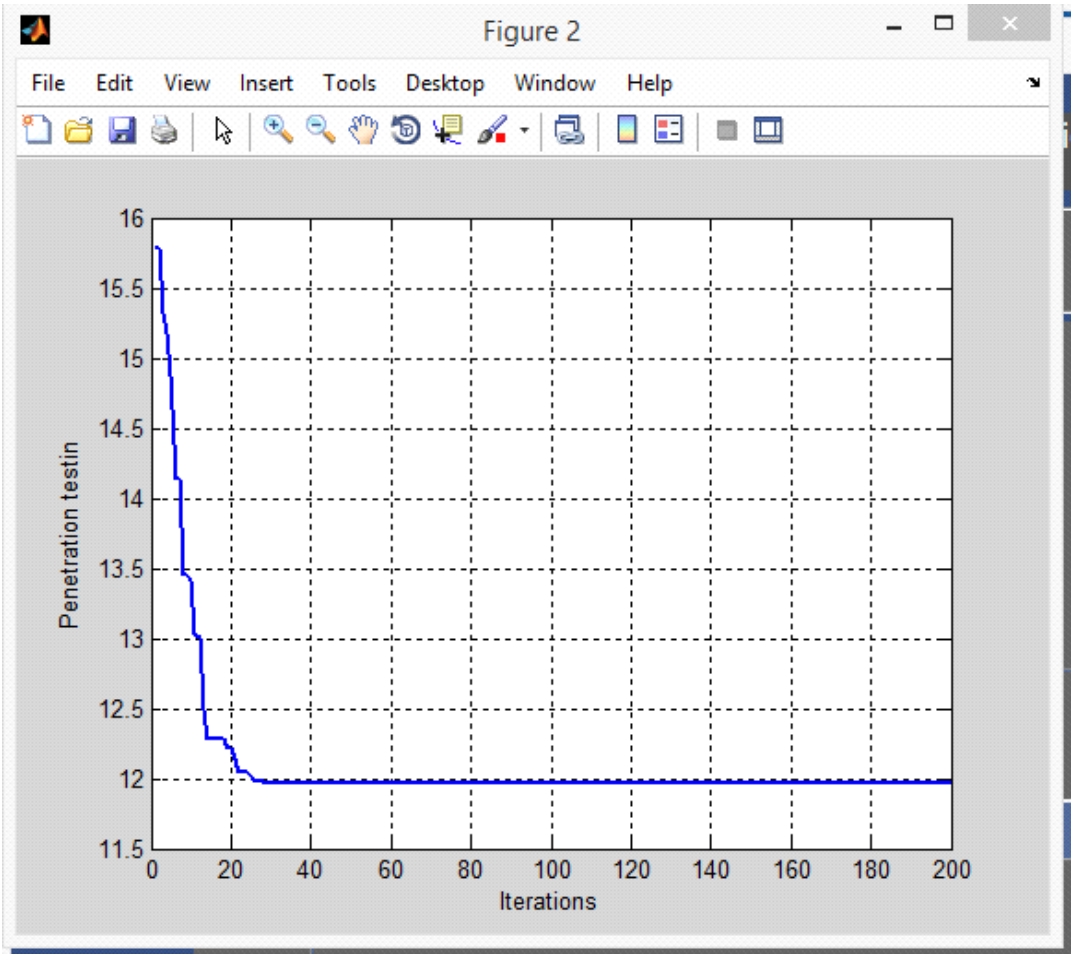

Figure 4.3 Plotting of the best values

As shown in the figure 4.3, the cost of penetration is examined through considering every character of network. Every value of each iteration is plotted in the shown line graph.

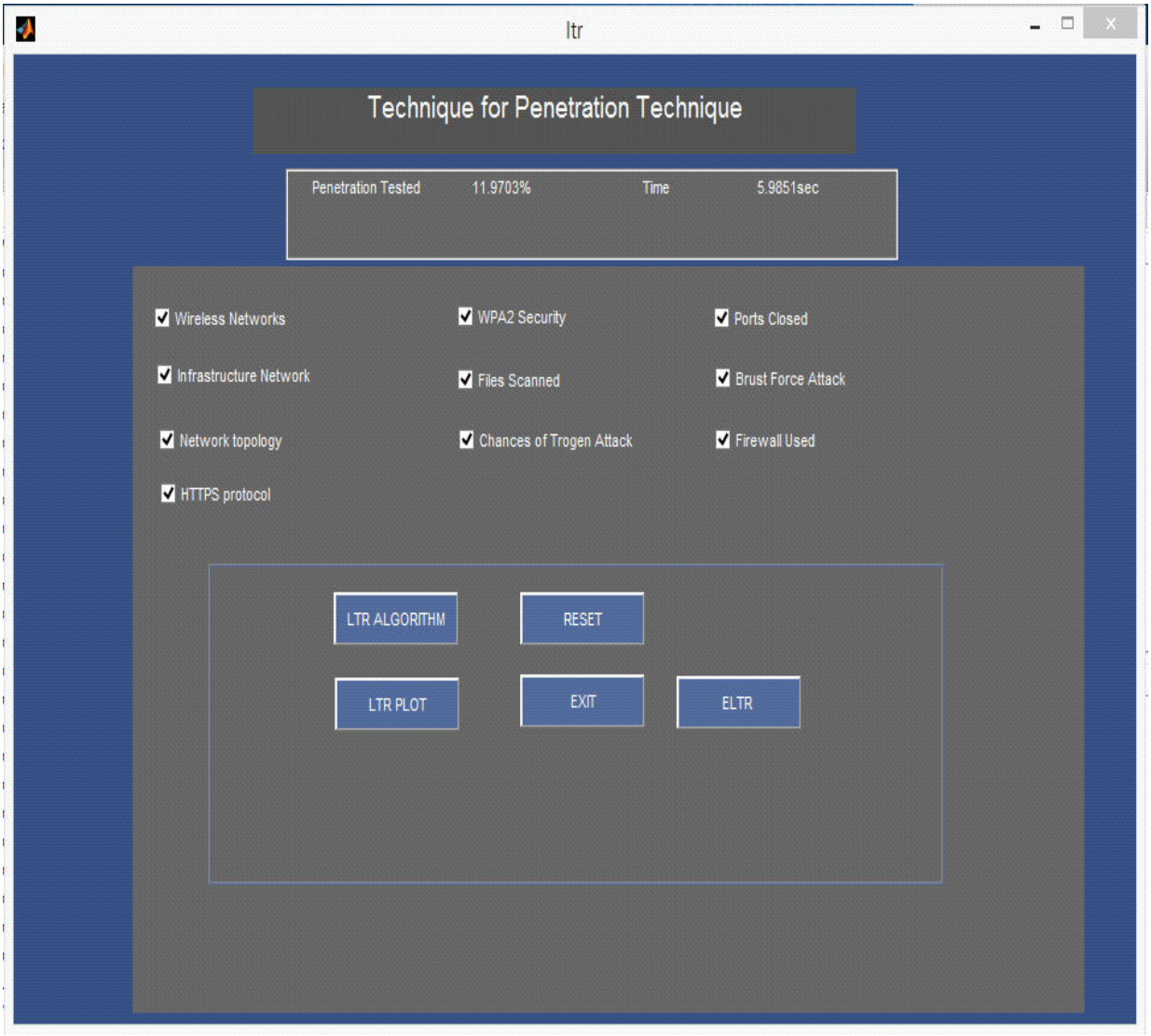

Figure 4.4 Default interface of proposed Technique

As shown within the figure 4.4, the default interface is designed in which the improvement is carried out the usage of the lower back propagation set of rules in the present method

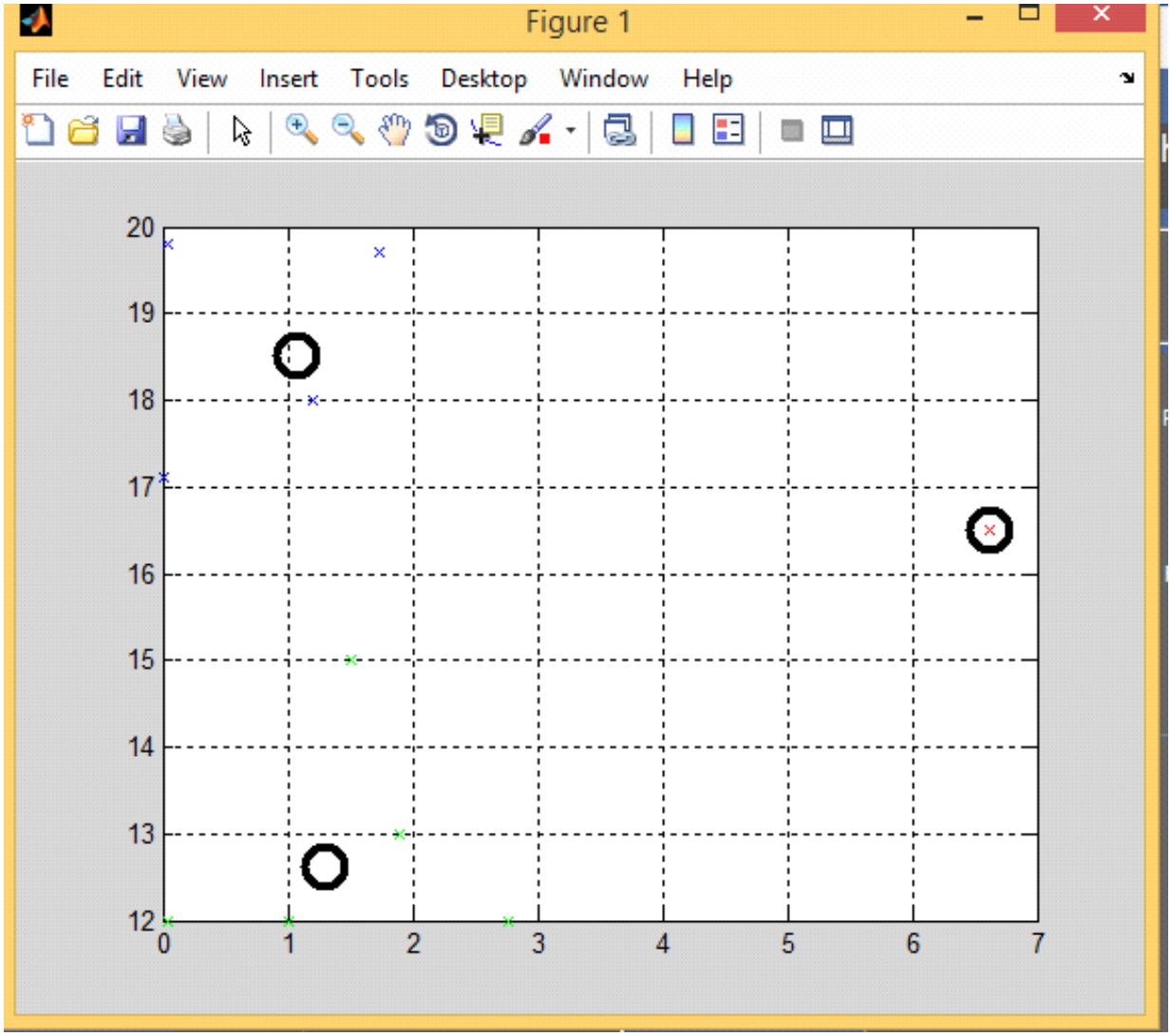

Figure 4.5 Plotting of iteration values

As shown in the figure 4.5, the proposed technique is primarily based on back propagation set of rules that is applied with the analyze-to-rank algorithm. The value of each iteration is proven in the figure

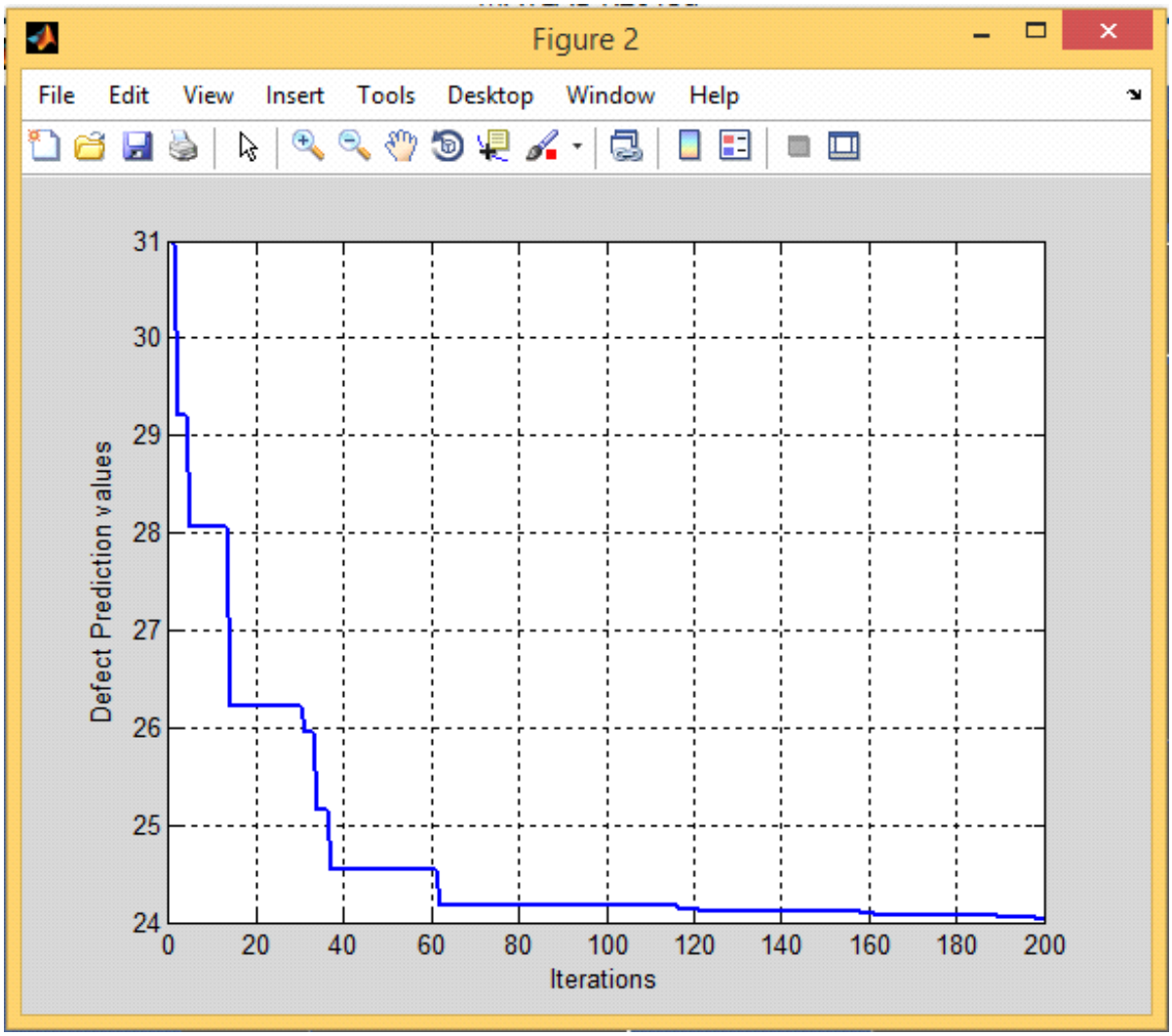

Figure 4.6 Plotting the values of each iteration

As shown inside the figure 4.6, the technique of back propagation is implemented with the examine-to-rank algorithm. The value of every new release is plotted with the line graph

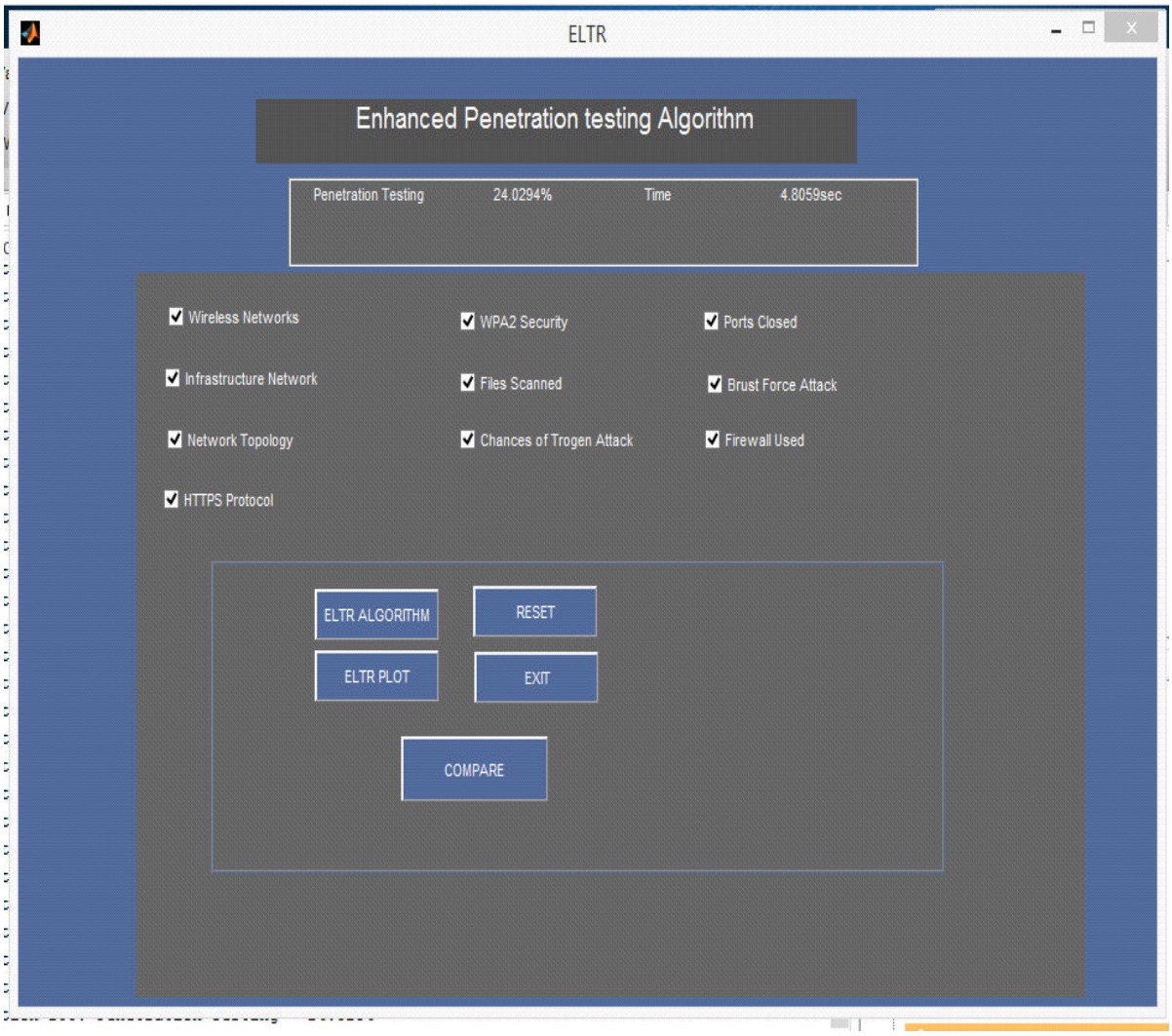

Figure 4.7 Display value of discover penetration testing

As shown in the figure 4.7, the algorithm of rank-to-study is carried out with the lower back propagation which discover on the penetration method and also the execution time is proven inside the figure

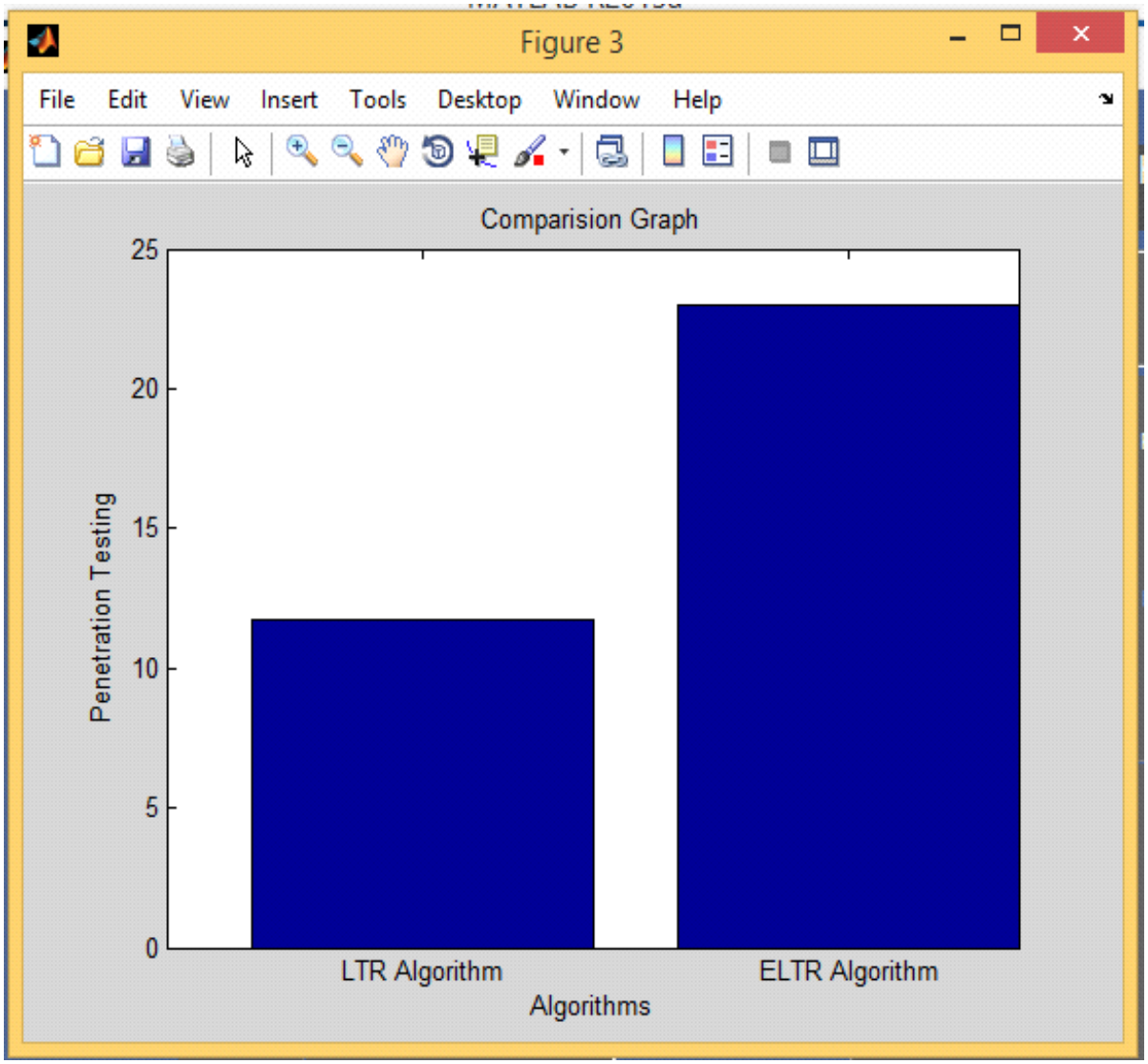

Figure 4.8 Penetration comparison

As proven inside the figure 4.8, the contrast among the current learn-to-rank algorithm and enhanced learn-to-rank algorithm is done. It is been analyzed that more suitable algorithm stumble on more quantity of penetration value than current one

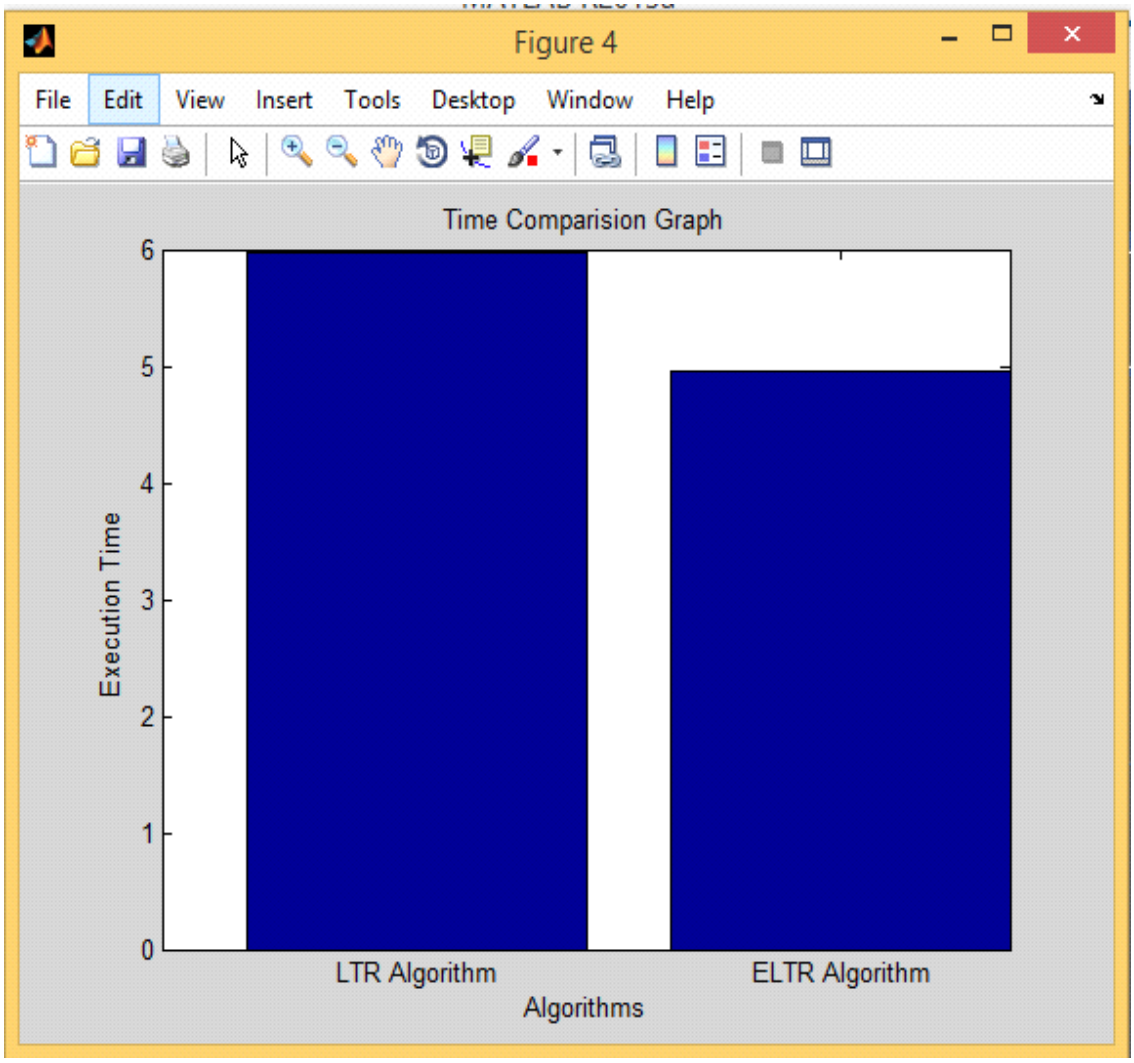

Figure 4.9 Time comparison

As proven inside the figure 4.9, the execution time of the present lean-to-rank algorithm is completed greater than enhanced learn-to-rank algorithm

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In this work, it's been concluded that penetration is the form of testing that's used to hit upon vulnerability and security flaws from the software program. The technique of research-to-rank is been implemented which locate the penetration value from network. In the learn-to-rank set of rules rating to every features of the software program is accomplished that's used to locate penetration cost of the network. In this work, back propagation algorithm is used with the research-to-rank set of rules to increase the penetration value of the network. It is been analyzed that penetration value of the proposed set of rules is increase upto 20 percentage and execution time is decreased to 15 percent .

5.2 Future work

Following are the various future protectives of this research work

1. The proposed algorithm can be further improved to analyze the penetration value of the network as the execution time .

2. The proposed algorithm can be compared with the other penetration algorithm to analyze its reliability.

REFERENCES

I. Research Papers

[1] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Kim, T., "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks", 2009, IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6

[2] Hayajneh, T.; Almashaqbeh, G.; Ullah, S., "A Green Approach for Selfish Misbehavior Detection in 802.11-Based Wireless Networks", 2015, Mobile Netw. Appl. 20, 623–635

[3] Panyim, K.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D., "On limitedrange strategic/random jamming attacks in wireless ad hoc networks", 2009, IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23, pp. 922–929.

[4] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Le, A., "Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies", 2012, Mobile Netw. Appl. 17, 415–430

[5] Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Deworm, "A simple protocol to detect wormhole attacks in wireless ad hoc networks", 2009, IEEE 3rd International Conference on Network and System Security, Gold Coast, Australia, 19–21, pp. 73–80

[6] Hayajneh, T.; Doomun, R.; Krishnamurthy, P.; Tipper, D., "Source— Destination obfuscation in wireless ad hoc networks", 2011, Secur. Commun. Netw. 4, 888–901

[7] Doomun, R.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Secloud:, "Source and destination seclusion using clouds for wireless ad hoc networks", 2009, IEEE Symposium on Computers and Communications, Sousse, Tunisia, 5–8 July pp. 361–367

[8] T. Hayajneh, S Ullah, BJ Mohd, K. Balagani, "An Enhanced WLAN Security System with FPGA Implementation for Multimedia Applications," 2015, IEEE Systems Journal

[9] T. Hayajneh, R. Doomun, G. Al-Mashaqbeh, BJ Mohd "An energyefficient and security aware route selection protocol for wireless sensor networks," 2014, Security and Communication Networks, John Wiley, Vol. 7, No. 11, pp 2015-2038

[10] Bassam J. Mohd, Thaier Hayajneh and Athanasios V.Vasilakos, “A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues”, 2007, Journal of Network and Computer Applications

[11] Bassam J. Mohd, Thaier Hayajneh and Athanasios V.Vasilakos,,” A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues”, 2009, Journal of Network and Computer Applications

[12] T. Hayajneh, BJ Mohd, A. Itradat, AN Quttoum, “Performance and Information Security Evaluation with Firewalls,” 2013, International Journal of Security and Its Applications, SERSC, Vol. 7, No. 6, pp 355-372

[13] Timothy C.Lethbridge,Robert Langaniere, “Object oriented software Engineering practical software development using UML and java”, 2001, Tata McGraw Hill Eduction Private Limited.

[14] Gregg Rothermel,Roland H.untch,Chengyun Chu, “prioritize the test case for Regression testing”, 2001, IEEE Transactions on Software Engineering

[15] Hema Srikanthi,Laurie williamsi,Jason Osborne, “system test case prioritization of new regression test case”, 2000, IEEE

[16] Sebastian Elbaum, Gregg Rothermel,*y* Satya Kanduri,*z* Alexey G. Malishevsk, “Selecting a Cost-Effective Test Case Prioritization Technique”, 2004, IEEE

[17] Lingming Zhang, Ji Zhou, Dan Hao ,Lu Zhang, Hong Mei, “Prioritizing JUnit Test Cases in Absence of Coverage Information”, 2009, IEEE .

[18] Paolo Tonella, Paolo Avesani, Angelo Susi, “Using the Case-Based Ranking Methodology for Test Case Prioritization”, 2009, 22nd IEEE International Conference on Software Maintenance (ICSM'06)

[19] Zheng Li, Mark Harman, and Robert M. Hierons, “Search Algorithms for Regression Test Case Prioritization”, 2007, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 33, NO. 4

[20] Praveen Ranjan Srivastava, “TEST CASE PRIORITIZATION”, 2008, Journal of Theoretical and Applied Information Technology

[21] Ruchika Malhotra, Arvinder Kaur and Yogesh Singh, “A Regression Test Selection and PrioritizationTechnique”, 2010, Journal of Information Processing Systems, Vol.6, No.2

[22] Matthew Denis, Carlos Zena, Thaier Hayajneh, “Penetration Testing: Concepts, Attack Methods, and Defense Strategies”, 2016, IEEE

[23] Jai Narayan Goel, Mohsen Hallaj Asghar, Vivek Kumar, Sudhir Kumar Pandey, “Ensemble Based Approach to Increase Vulnerability Assessment and Penetration Testing Accuracy”, 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[24] Herny Ramadhani Husny Hamid, Megat Ahmad Izzat b Megat Ahmad Kamil, Norhaiza Ya Abdullah, “Portable Toolkit for Penetration Testing and Firewall Configuration”, 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic

[25] A. K. Pathak, Dr. M. P. Sharma, Dr. Manoj Gupta, “Modeling and Simulation of SVC for Reactive Power Control in High Penetration Wind Power System”, 2015, IEEE

[26] Marri Rami Reddy, Dr. PrashanthYalla, “Mathematical Analysis of Penetration Testing and Vulnerability Countermeasures”, 2016, 2nd IEEE International Conference on Engineering and Technology (ICETECH)

[27] Kamran Shaukat, Amber Faisal, Rabia Masood, Ayesha Usman, Usman Shaukat, “Security Quality Assurance through Penetration Testing”, 2016, IEEE

[28] Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar, “Cyber Security Analysis using Vulnerability Assessment and Penetration Testing”, 2016, IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16)

[29] Siripong Roongrungsuwan, Jirapun Daengdej, “TEST CASE PRIORITIZATION TECHNIQUES”, 2010, Journal of Theoretical and applied information Technology, JATT&LLS

[30] Hyunsook Do, Siavash Mirarab, landanTahvildari, and Gregg Rothermel, “The effect of time constrainton test case prioritization”, 2010, IEEE TRANSACTION ON SOFTWARE ENGINEERING ,VOL.36

[31] Alien G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, “Overview of Penetration Testing”, 2011

[32] Konstantin us Xynos, Iain Sutherland, “Penetration Testing and Vulnerability Assessments: - A Professional Approach”, 2010

[33] Network Penetration Testing and Research Brandon F. Murphy, 2013

[34] Emily Chow, “Ethical Hacking and Penetration Testing ACC626:- IT Research Paper”, 2011

[35] Len Klein man, “Vulnerability Management and Research Penetration Testing Overview”, 2013

[36] Parag Pravin Shimpi, Sangeeta Nagpure, “Penetration Testing:- An Ethical way of Hacking”, 2015

[37] Gordon Fraser, “Tunneling, Pivoting and Web Application Penetration Testing”, 2015

[38] Maxim Catanoi, “Penetration Testing: Alternative to Password Cracking”, 2015

[39] Matt Koch, “Web Application File Upload Vulnerabilities”, 2015

[40] Andrew Andrasik, “In but not Out: Protecting Confidentiality during Penetration Testing”, 2016

[41] Jianming Zhao, Wenli Shang, Ming Wan, Peng Zeng, “Penetration Testing Automation Assessment Method Based on Rule Tree”, 2015, the 5th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems

[42] Suyash Jadhav, Tae Oh, Young Ho Kim, Joeng Nyeo Kim, “Mobile Device Penetration Testing Framework and Platform for the Mobile Device Security Course”, 2015, ICACT

[41] Surya Michrandi Nasution, Yudha Purwanto, Agus Virgono, M. Rifqi Y. Tambunan, “Integration of Autonomous Sender for Hidden Log Data on Kleptoware for Supporting Physical Penetration Testing”, 2015, IEEE

[43] Surya Michrandi Nasution, Yudha Purwanto, Agus Virgono, M. Rifqi Y. Tambunan, “Integration of Autonomous Sender for Hidden Log Data on Kleptoware for Supporting Physical Penetration Testing”, 2015, IEEE

II. Websites

1. www.pen testeracademy.com
2. https://pentest-tools.com
3. https://pentestmag.com
4. www.pentest.co.uk
5. http://www.computerweekly.com
6. https://link.springer.com
7. https://www.tutorialspoint.com

.