

Research Proposal

by Rumen Chowdhury

FILE	2943_RUMEN_CHOWDHURY_RESEARCH_PROPOSAL_93935_660430660.DOCX (444.49K)		
TIME SUBMITTED	08-MAY-2019 11:31PM (UTC+0100)	WORD COUNT	5230
SUBMISSION ID	106705011	CHARACTER COUNT	29164

Evaluation of a Portable Penetration Within a Communication System (May 2019)

Rumen Chowdhury

Student No. P146446

Module Code: M7X01691

Computer Networks and Security

Dr. Mabrouka Abuhmida

Dr. Nik Whitehead

Research Methods

Email: Mabrouka.abuhmida@uwtsd.ac.uk

Abstract—The concept of Penetration testing explains the process of adopting techniques of attacking a targeted system or network using automated tools or manual penetration. The primary aim of Penetration Testing is to discover the maximum vulnerabilities. After comprising the targeted network, it is best practice to produce a solution to each vulnerability discovered, this in turn provides the company with an enhanced prevention of security threats. This paper will propose the various ways to carry out Penetration Testing and validate each process. The concepts of data confidentiality, availability and integrity come into play when dealing with security considerations. The principles of ethical hacking are presented with a professional methodology approach.

Index Terms—Penetration Testing, System, Network, Vulnerability, Security Threats, Confidentiality, Availability, Integrity

Figure 1 - Comparison between Raspberry Pi & Desktop.....	3
Figure 2 - IBM AppScan	3
Figure 3 - Nessus	3
Figure 4 - NMAP	3
Figure 5 - Penetration Areas	4
Figure 6 - Penetration Testing Phase	5
Figure 7 - Gantt Chart.....	7

I. INTRODUCTION

THIS paper introduces the fundamental aspects and principles of research methods and data analysis in relation to a chosen field of interest. The author shall present the ideologies of research purposes and approaches to carry out a research proposal. The author shall create a research proposal with a topic of interest. In order to generate this, the author will sufficiently generate a level of innovation and originality when gathering sources of relevant information while considering the validation of each process. Primarily, the focal point of this paper resides to portable penetration testing with an analyzed comparison of traditional penetration testing to evaluate the differences between each method, this in turn will provide the best alternatives to security testing and ensuring integrity on industrial networks.

The conception of vulnerability testing provides substantial benefits to corporations to maximize protection. To test one's own network integrity is more beneficial than employing professional to carry out the security checks, this way the assurance of data protection and personnel is safeguarded. Through regular procedures of vulnerability testing, corporations can remain adamant about one's own assets and monitor the performance while considering each network end point and crucial information[1]–[9].

II. AIMS & OBJECTIVES

To interpret simply, the aim of the research proposal is to demonstrate an understanding to carry out an automated portable network penetration testing towards a university network. To gain a deeper understanding, the author will explain the necessary literature of what of Penetration Testing stands for. The purpose of this proposal is to initially gather the research required for implementation. The practical development involves the use of a Raspberry Pi device to carry out the penetration testing.

The author will develop a structural guideline to follow in order to carry out successful implementation. There will exist an explanation of each objective to gain a knowledgeable criterion to abide by, therefore the reader also receives an understanding of the methodology approach the author intends to follow. The author provides a list of the objectives below:

- Review possible up to date technologies that provide any advantage to penetration testing
- Identify current security methods which can perform penetration implementation
- Isolate portable penetration testing methods as well as traditional methods
- Identify possible differences with portable penetration testing and traditional
- Evaluate the differences between the testing methods performed

III. RELATED WORK

The author introduces the concepts of alternative methods to Penetration testing such as portable techniques. The main research literature the author intends to propose is the concepts of portability approaches over conventional approaches. This ideology has become quite mainstream due the advantages it provides such as portability, cheaper implementation, less operational power and many others. The benefits of penetration prove to be a valuable advantage to many concepts of legality, reduced costs, remediation and recuperation[10], [11].

Corporations should employ training systems for each staff of the I.T department, this way the company can support self-sufficiency of the network infrastructure by learning how to perform vulnerability assessments, this way the employees of each company become professional themselves. The employees begin to understand how to defend assets such as company applications, services, network and users of internal and external end points, this in turn allows each staff to provide an input into the analysis of the reports and reach a conclusion[12]–[14].

The cost of maintenance of security services and application can be quite expensive in the event of a network breach and data loss, the company must attempt to recover from these attacks as soon as possible, this can be costly for the company to recover the loss that has occurred, therefore financially security breaches prove to be expensive. Company reputation be also being at stake as well as financial implications, in the sense of losing customer loyalty and legal activities. Penetration Testing can aid in avoiding these complications listed above by proactively attempting to maintain security checks, this way the company can be given the ability to protect the confidentiality, availability and integrity of the network infrastructure[15]–[18].

Evaluation of Portable Penetration Testing on Smart Cities Applications using Raspberry Pi III (2017)

This paper proposes the idea of introducing the concept of a smart solution to penetration testing performed for smart cities. The idea comes into existence by utilizing the components of a Raspberry Pi, which is essentially a mini computer capable of performing a variety of functions and tasks of computing as well as programming. In this case, the portable device can be programmed to complete tasks such as penetration testing and discovering possible vulnerabilities a security audit can find, therefore this is purpose of this paper the author discusses. The author explains the explains and evaluates the benefits of introducing the idea of portable penetration testing and vulnerability assessments[19].

The aim of this paper evolves around the effectiveness of utilizing a portable device such as a Raspberry Pi to perform penetration testing towards a smart environment. Due to the security threats a smart city may be bound by, the author developed a solution to this problem as there a substantial

number of vulnerabilities that affect smart cities. The overall objective evaluated how effective the Raspberry Pi was at discovering these vulnerabilities. A smart solution which can successfully carry out the vulnerability assessments which can be of benefit to industrial networks, organizations which utilizing smart cities and other applications[19].

The research aimed to answer various question which would clarify the proposal introduced. Some of the questions involved the production of a portable device, was it possible to utilize a Raspberry Pi to carry out penetration testing towards smart devices. What results can be discovered from the portable penetration testing. Do the benefits of utilizing the Raspberry Pi outweigh the methods of traditional approaches such as via a desktop? How do the results of the portable penetration test compare to the implementation of traditional methods? Finally, how can the process of penetration testing further exist to develop[19].

In order for the user to operate this procedure, the Raspberry Pi required the necessary software implementation, in this case the operating system used was Kali Linux, which proves to exist as a power operating system perform vulnerabilities assessments. With this software, the user is granted an abundance of added tools which perform various other vulnerabilities assessments. The researcher uses these tools to execute a vulnerability analysis[19].

The implementation existed as a two-part development, meaning that the author utilized the portable penetration as well as a desktop implementation to compare the results as mentioned within the literature. The author displays the results from the running scans along with the comparison of the two methods of testing;

TABLE 1. COMPARISON BETWEEN PEN-TEST VIA DESKTOP VS. PEN-TEST VIA RASPBERRY III [11]

	Penetration testing via desktop	Penetration testing via Raspberry III
Equipment	High performance computer	- Raspberry Pi III device - Kali operation system or Raspian. - Vulnerability Assessment program licenses.
Operating System	- Licensed OS	Open source OS such Kali Linux OS or Raspian.
Vulnerability Assessment Tools	- VMware license - Vulnerability Assessment program licenses.	Built-in open source vulnerability assessment tools in Kali
Price	start from 8200\$	The cost of Raspberry device is around 64\$, other cost may be added for the licensed scanners such as "IBM Appscan license"
Expertise	More expertise who deals with computers.	Staff training, require basic skills in how to install and use the programs.
Portable	No	Yes
Operation	More labs = more operation power.	No labs = less operation power.

Figure 1 - Comparison between Raspberry Pi & Desktop

The author illustrates the comparison between both devices, considering each element of functions which can be achieved.

TABLE 2. IBM AppScan Scanner's Result

Vulnerability Assessment	Number of issues	High	Moderate	Low
Via Laptop	55	3	10	1
Via Raspberry	55	3	10	1

Figure 2 - IBM AppScan

Here the author displays the results from the IBM scans, which was run on both devices, the reader could clearly see the output, which suggests the Raspberry Pi works just as well as a traditional method.

TABLE 3. NNESSUS SCANNER'S RESULT

VA	# of vulnerabilities	Type of vulnerability	High	Moderate	Low
Via Laptop	3	•SSL 64-bit Block Size Cipher Suites Supported (SWEET32). •SSL Certificate Cannot Be Trusted. •SSL Medium Strength Cipher Suites Supported.	NA	3	NA
Via Raspberry	3	•SSL 64-bit Block Size Cipher Suites Supported (SWEET32). •SSL Certificate Cannot Be Trusted. •SSL Medium Strength Cipher Suites Supported.	NA	3	NA

Figure 3 - Nessus

The above image displays the results from the Nessus vulnerability scanner, from the output shown, the viewer can visually read the similarities shown.

Table 4. NMAP RESULT

Vulnerability Assessment	Open Port	Closed Port	Running Services	Identify OS
Via Laptop	✓	✓	✓	✓
Via Raspberry	✓	✓	✓	✓

Figure 4 - NMAP

The author displays the running scan of NMAP, which is a network discovery tool, the illustrations, proves that both methods can find the different type of services, which are listed within the table.

Evaluation – to conclude the author carried out two penetration testing assessments via portable device of Raspberry Pi and Laptop. The data was analyzed and compared against to discover potential differences in assessments. The author came to a finding to clarify that the portable a portable device such as a programmable Raspberry Pi was able to function as a penetration testing tool. This benefits the users as it provides a low-cost solution to vulnerability assessments as opposed to traditional methods of using a computer which requires more operational power. The Raspberry Pi works well and aids the pen tester with an abundance of tools to utilize in performing security testing and auditing methods, this in turn reduces the cost of exploitation and installation. The alternative methods of penetration testing proved to be resourceful, therefore the author recommends a regular security check and provide a full audit into reports to analyze each assessment[19].

Portable Toolkit for Penetration Testing and Firewall Configuration (2015)

This paper introduces the idea of portable penetration within a security testing environment. This device proposed was named Portable Penetration Testing and Firewall Configuration Toolkit, developed to allow users to carry out a simulated penetration testing and also configure a firewall on the portable device. The author utilizes the device of a Raspberry Pi which was mentioned in the previous paper, this allows to create and program the device to perform designated operations.

The author gathers the necessary software requirements needed to produce a penetration testing framework, taking into account the relevant operating system, tools required to perform vulnerability assessments and the hardware equipment to manufacture the entire device. In this the case, the author utilized a Raspberry Pi with the Kali Linux operating system, this distribution proves to exist as one of the most reliable systems for conducting security analysis. The additional software tool which the author implemented within the Raspberry Pi was a firewall configuration tool, an open source distribution called IPFire, which allows users to modify the Raspberry into a configurable firewall, as a testing environment it will provide a security protection between its connected

interfaces such as between a router and end device, thus users will be granted a small physical firewall[20].

Following on, the author provides some research based on current technologies produced which also provide users with a portable penetration testing framework. This provides the reader with an insight into what alternative methods users can perform and which tools can be utilized to produce vulnerability assessments. The comparison involves characteristics of hardware and software differences such as cost, network requirements, storage and other physical characteristics[20].

Evaluation – the author concludes by evaluating the concepts of portable penetration testing and firewall configuration environment. The disadvantage of this proposal is that it is only still in experimental phase towards a educational background, thus the method of testing is limited for usage, however the principle remains the same, the ability to carry out portable penetration testing with alternatives such as firewall configuration using Raspberry Pi. To further develop this, the author recommends the producer to create a solid portable penetration testing framework[20].

A Study on Penetration Testing Process and Tools (2018)

As the author introduced the concepts and principles of portable penetration testing, it was relevant to mention the aspects of traditional penetration methods and the types of penetration assessments that be carried out. This paper evaluates the various approaches with penetration testing process and procedures while considering the benefits it provides towards industrial organizations as well the ethical complications involved[21].

This author begins by discussing the corporate data and information that is of utmost importance within organizations. If there is no security compliance within businesses, there is no values to be held for that business, information should be protected as all cost following correct and relevant procedures for protection following standards of ethical value. The author has mentioned the concept of traditional penetration testing, it is a vulnerability assessment that is conducted towards a targeted system, considering software, hardware, operations, weakness and many other factors. To pen test against one's own network means to test the level of security integrity of that system which hackers may aim to achieve[21].

In an ethical environment, a penetration test is conducted by a professional to identify possible vulnerabilities that may exist within a network, with permission, the ethical hacker is given the opportunity to attack the targeted system utilizing an abundance of an arsenal. The author mentions the objectives of Penetration Testing and importance it may have towards organizations. To create security awareness at various levels of the company through repetitive training modules, this in turn allows the company to build a strong IT infrastructure and avoid information and financial loss. To test against the integrity of

each system and existing security policy, it aids the decision to further develop a IT security improvement[21].

There are three main types of penetration methods which the author mentions, these are Black Box, White Box and Grey Box testing. In a black box testing environment, a user retains no knowledge of any events towards the targeted system, therefore each step is learning approach from the start. A white box penetration testing is the approach given to the user while considering all the information that is provided, therefore further vulnerabilities discovered are new. A grey box pen tester has only established partial information of the intended target while identifying further vulnerabilities. A pen tester may have conducted these tests via inside or outside the network, this is known as external and internal testing, both provide the relevant advantages such as via internal, the tester is given the inside credentials and privileges already, whereas external testing allows the company to view the possible vulnerabilities a hacker may discover through outside methods[21].

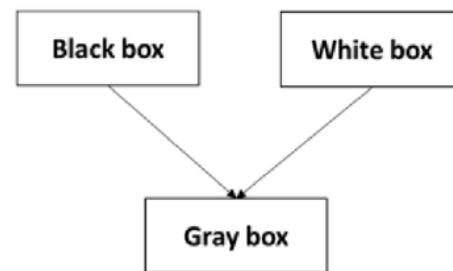


Figure 5 - Penetration Areas

The author further explains the variations of penetration testing that can be conducted towards a target. A user is able to test against router security for certain vulnerabilities that may occur such as configuration errors. A router may be misconfigured, which in turn allows hackers to take advantage of this by sending malicious traffic across the network. This method can identify the possible misconfigurations and reconfigure the correct implementations within that router. Application penetration can be relevant to conduct due to the vulnerabilities applications can possess such as programmable errors and backdoor vulnerabilities, applications may be connected to operating systems and backbone network, thus this provides an exploit for hackers. Intrusion Detection Systems may provide substantial security for companies but there are also weak IDS that are implemented, this in turn allows hackers to discover look holes within the system, the typical IDS configuration can be easily bypassed by experienced hackers. There are many other variations such as password cracking and social engineering penetration[21].

Following on, the author introduces the penetration testing process, procedure, and documentation with a systematic approach based on each phase. Below, the author provides the penetration testing model intended to validate the testing.

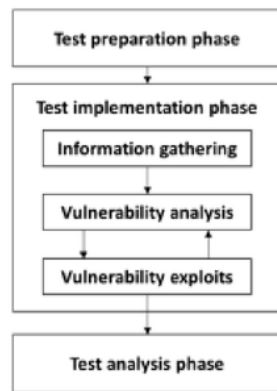


Figure 6 - Penetration Testing Phase

Above the author provides the test phases for conducting a penetration test. The first step is called the preparation phase, this is process of gathering and collected the aim and objectives are identified. Specific aspects are also gathered such as network downtime and information outflow as well as legal agreements. Moving on to the main section of the penetration testing, the author begins the test information phase, the information gathering stage involves identifying and scanning the topology of the target required for the vulnerability analysis. Based on the vulnerabilities discovered, the tester begins to run automated or manual penetration testing techniques. The tester utilizes the concept of code analysis, which involves discovering security flaws by identifying source code. Within the vulnerability analysis phase, the tester presents the idea of vulnerability discovery, which involves discovering and understanding the vulnerabilities, this in turn allows engineers to mitigate further attacks that may occur. Following on the vulnerability exploits phase, using the information discovered, the tester exploits the further vulnerability analysis[21].

The final stage of the penetration testing model is the testing analysis phase; this is where the completion of the vulnerability analysis is compiled into reports and documentation and sent to senior management. The report contains technical assessments of the vulnerability exploits discovered which the IT staff would possibly understand, there will be areas covered that should highlight different aspects of the exploits including findings, patch updates, costing and time estimation evaluation. The author concludes by mentioning the penetration testing tools that can be utilized;

- NMap, BeEF, Metasploit, Nessuss, Cain and Abel

IV. RESEARCH METHODS

This section clarifies the principles of research methodology which the author wishes to progress on and follow. Research methodology becomes relevant to a professional by allowing researchers to gather designated information and data to suit the

needs and requirements of the project. There are various ways to gather this information such as surveys, interviews and questionnaires to represent the information being collected. This benefits the researcher to further study the topic intended to conduct which provides a proficient approach, this enables the researcher to gain control of the intended literature to suit the needs and requirements of the study. It offers the ability to apply the suitable methods of qualitative or quantitative research. The author proposes a professional body of research methodology to provide the reader with the approaches intended to complete the research proposal. Below the author provides each approach intended to take based on a professional body study, the research onion. The methodology which the author shall discuss refers to the techniques intended to gather information and the process of representing the analytical data[11].

A. Philosophy

The research philosophy provides the reader with the advance of the reality of the methodology therefore this creates a validation for the process of the research. Based on the research onion, the author intended to conduct the approach of a Positivism, this approach allows the author to test a hypothesis set out to be measured and analyzed. The information gathered from a positivism approach allows the research to test real world hypothesis to generate the same or different results, due to the data being quantifiable, this provides the ability to perform statistical analysis[11].

B. Approaches

The research approach allows the author to follow either a deductive or inductive method, this is also based on the previous research philosophy decisions which are made by the researcher. The approach which the author intends to follow is the deductive approach, this method allows formulation of an existing hypothesis and reach a conclusion of validation. A formulated research question which is extracted from a hypothesis to answer questions set out by the researcher. To validate the research approach, the author intends to take a deductive approach as it meets the required brief[11].

C. Strategies

Following on from the previous research methodology, as the author has established the method approach intended to take, the next process would be to establish the way the approach would be conducted. The research strategies refer to the collection of the intended data or information, there are various ways to decide this method as long the end justifies the mean. In this case, the appropriate measure would be to test an experimental approach. by deciding on an experimental approach, the author is able to carry out a physical structure of design and create statistical data to be analyzed[11].

D. Time Horizons

In order to establish the correct proceedings for the research methodology, the author must decide the time horizons which are appropriate for conducting. There are two different options the author can undertake, these are longitudinal and cross-sectional, in simple terms cross-sectional is short term study and longitudinal is long term study. In this case the experiment may prove to extend for a long period of time, therefore it would be sufficient for the author to conduct a longitudinal study. A penetration testing assessment may take as long as days to discover vulnerabilities depending on the target system, thus this provides the author with different measures of testing[11].

E. Data Collection & Evaluation

After deciding upon the methods of study to be taken, the author shall finally come to a decision for information gathering or data collection. The data collection method necessitates an analytical concurrence to the research approach. This decision incorporates the research design overview, as the correct approach for data collection will work best for the suitable research proposal, which the results will be analyzed accordingly to answer any statements made. The information gathered will be evaluated accordingly[11].

F. Risks and Limitations

The author intends to conduct an experimental approach to the research proposed, in turn the information gathered would be analyzed into statistical data for questioning. The author may reach an impasse in which the breach of limitations and risks appear. There are always complications when conducting a project or research proposal, these are typically aspects where the author cannot either comprehend or overcome due to unforeseen or potential end. This may not be seen as a downfall for the author as further research could be conducted by other researchers to explore various areas around the limitations.

V. DEVELOPMENT METHODS

The developmental methods the author conducts and proposes are the aspects of the research which is defined, such as the way the research will be conducted. The relevant research approaches will share focus on the descriptive knowledge intended to gather, which in turn allows the researcher to answer appropriate statements. Overall the development methods shall define the whole research methodology and govern the body of descriptive knowledge of hypothesis of the tested design principles. The author shall discuss any other relevant development methods within this section.

A. Software Development

Following on from the previous section of development methods, the author extends the research approach by mentioning the scientific and technical methods of conducting the experimental design. The software development or

specification will define the characteristics of the project development. The author will decide on the relevant software requirements based on the design to be implemented. Due to the field of study being wide, the author is presented with various tools to carry out a penetration testing assessment, which in turn will provide the reader with the necessary knowledge of expertise.

B. Research deliverables

The author intends to validate the research proposal by providing an outcome for the project; this can be aspects of benefits, the reason for the project, the outcome, what is intended to gain out of the implementation. Due to the nature of the project, the emphasis on the portability will be explained and the author shall reach a conclusion to decide on the actions to take. The reason for this being, the project shall give some recognition and benefit to the university. The author intends to display the running outcome into reports and audits to finalize the analyzed data.

VI. RESOURCES & PLANNING

The author provides the necessary information for the production of the resources and planning to identify the potential areas of development. The knowledge of resources and planning shall define the design and implementation and provide a validation for the formulation of the research. The resources intended to be involved within the implementation shall be thoroughly explained to provide the reader with a descriptive analysis, therefore this will justify the procedure for planning and execution. The planning procedure will validate the authors approach of the method of research proposed.

A. Resources Required

After providing the relevant information for the planning procedure, the techniques and tools shall be justified with the selection of experimental approaches. The relevant resources required will provide a validation to the research in the case of success. The applicable resources required will be built in software within the operating system of Kali Linux, this allows the user to test out the current tools and further gather resources to allow further development. The author provides a thorough list of the resources required for the project:

- A programmable device capable of carrying out the operations of penetration testing (Raspberry Pi).
- The equipment required to build the Raspberry Pi (Battery pack, Wi-Fi card, SD card, Mini touch-screen monitor, Bluetooth keyboard).
- The relevant plan and procedure to conduct the experiment.
- A specialized operating system to provide the basis of the model (Kali Linux).
- A variation of the specialized software tools required to conduct the experiment.

B. Gantt chart

After careful considering on the research methodology approaches and techniques, the author intends to produce a visual representation of the timescales that were approached. It is best practice to implement this procedure to provide the reader with the duration of the research proposal, considering the time schedules involved and each step within the process. It provides clarity over the entire project completion by viewing where each step has taken place and understand progression of each task. By being creative with the Gantt chart provides coordination to project managers to sequence the events taken place, this helps avoid any overloading. The disadvantage of this Gantt chart at this stage is the uncertainty of duration and completion for the project after the research proposal is completed. Below the author provides the screen shot for the Gantt chart;

Task Name	Duration	Start	Finish	Predecessors
• Research Proposal	90 days	Fri 04/01/19	Wed 08/05/19	
• Chapter 1 - Introduction	6 days	Mon 14/01/19	Mon 21/01/19	
Overview of research proposal	3 days	Mon 14/01/19	Wed 16/01/19	
Introduce the principles of penetration testing	3 days	Thu 17/01/19	Mon 21/01/19	4
• Chapter 2 - Aims & Objectives	4 days	Tue 22/01/19	Fri 25/01/19	
Established focal aim	2 days	Tue 22/01/19	Wed 23/01/19	
Established objectives	2 days	Thu 24/01/19	Fri 25/01/19	7
• Chapter 3 - Related Work	20 days	Tue 26/02/19	Mon 25/03/19	
Introduce the research literature	2 days	Tue 26/02/19	Wed 27/02/19	
Evaluation of Portable Penetration Testing on Smart Cities Applications using Raspberry Pi III	4 days	Tue 26/02/19	Fri 01/03/19	
Portable Toolkit for Penetration Testing and Firewall Configuration	4 days	Mon 04/03/19	Thu 07/03/19	11
A Study on Penetration Testing Process and Tools	4 days	Fri 08/03/19	Wed 13/03/19	12
Overview and Open Issues on Penetration Testing	4 days	Thu 14/03/19	Tue 19/03/19	13
• Chapter 4 - Research Methods	14 days	Wed 20/03/19	Mon 08/04/19	
Establish Research philosophy	2 days	Wed 20/03/19	Thu 21/03/19	
Establish Research approaches	2 days	Fri 22/03/19	Mon 25/03/19	16
Establish Research strategies	2 days	Tue 26/03/19	Wed 27/03/19	17
Establish Time horizons	2 days	Thu 28/03/19	Fri 29/03/19	18
Establish Data collection & evaluation	2 days	Mon 01/04/19	Tue 02/04/19	19
Establish Risk & limitations	2 days	Wed 03/04/19	Thu 04/04/19	20
• Chapter 5 - Development Methods	4 days	Mon 08/04/19	Thu 11/04/19	
Establish software development	2 days	Mon 08/04/19	Tue 09/04/19	
Establish research deliverables	2 days	Wed 10/04/19	Thu 11/04/19	23
• Chapter 6 - Resources & Planning	4 days	Thu 11/04/19	Tue 16/04/19	
Establish the resources required for implementation	2 days	Thu 11/04/19	Fri 12/04/19	
Creation of the Gantt chart	2 days	Fri 12/04/19	Mon 15/04/19	26
• Chapter 7 - Ethical Considerations	9 days	Tue 16/04/19	Fri 26/04/19	
Establish ethical approval from university EI Form	3 days	Tue 16/04/19	Thu 18/04/19	
Explain ethics of Data Protection Act 1998	3 days	Fri 19/04/19	Tue 23/04/19	29
Explain Computer Misuse Act 1990	3 days	Wed 24/04/19	Fri 26/04/19	30
• Chapter 8 - Conclusion	4 days	Fri 01/02/19	Wed 06/02/19	
Summarize the overall research	4 days	Fri 01/02/19	Wed 06/02/19	

Figure 7 - Gantt Chart

VII. ETHICAL CONSIDERATIONS

One of the major considerations and aspects to cover is the concepts of ethics and the implications that may occur during the process of implementation; this is why the author gains an ethical approval with the intended organization. Due to the author requiring access to penetrate the services and network, an ethical rights approval allow a user to conduct any ethical hacking, which the author intends to carry out. Regarding the ethical rights from the university, it is crucial that the author request an ethical approval form from the university to avoid any implications towards to project. The form required is

named 'PG2-E1 Application of Ethical Approval'. The author finally requires understanding other laws and regulations of third party organizations which abide with ethical rights, these are the Data Protection Act 1998, Computer Misuse Act 1990, Serious Crime Act 2015, Police and Justice Act 2006, Digital Economy Act and many other forms government regulations.

VIII. CONCLUSION

In conclusion, the author carries out a professional research proposal based on a selective hypothesis of choice; this hypothesis was to test the ability of an alternative method to penetration testing using a portable device of Raspberry Pi as opposed to traditional methods. The author shall gathered various research literature to gain the knowledge of expertise within the field and provide a principle of support for the hypothesis, while considering validation for each literature source discovered and evaluated. The aim and objectives of the proposed project have been clearly established by the author; therefore, the basis of the proposal was outlined. The research required a standard body of professional practice, which is where the research methodology arises, to follow a method of approaches and a philosophy of work enables the author to gain an understanding on the steps to take for completion. Finally, the author provides the necessary aspects of the work, which collate to the resources and methodology approach, therefore this, will explain the systematic procedures intended to pursue to create and implement the project. The time scales of the research proposal explains the completion of each step in relation to the time threshold.

REFERENCES

- [1] A. Shah, M. A. Alasow, F. Sajjad, and J. J. A. Baig, "An evaluation of software requirements tools," in *2017 IEEE 8th International Conference on Intelligent Computing and Information Systems, ICICIS 2017*, 2018, vol. 2018-January, pp. 278–283.
- [2] J. Alves-Foss and S. Barbosa, "Assessing computer security vulnerability," *ACM SIGOPS Oper. Syst. Rev.*, vol. 29, no. 3, pp. 3–13, 2004.
- [3] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *J. Comput. Virol. Hacking Tech.*, vol. 11, no. 1, pp. 27–49, 2015.
- [4] K. kaur Ankita Gupta, Kavita, "Vulnerability Assessment And Penetration Testing," *Int. J. Eng. Trends Technol.* 2013 ISSN 2231-5381, vol. 4, no. 3, pp. 328–333, 2013.
- [5] I. Yaqoob, S. A. Hussain, S. Mamoon, N. Naseer, J. Akram, and A. Ur Rehman, "Penetration Testing and Vulnerability Assessment," *J. Netw. Commun. Emerg. Technol. www.jncet.org*, vol. 7, no. 8, 2017.
- [6] J. Doshi and B. Trivedi, "Comparison of Vulnerability Assessment and Penetration Testing," *Int. J. Appl. Inf. Syst.*, vol. 8, no. 6, pp. 51–53, 2015.
- [7] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 Int.*

- Conf. Comput. Commun. Control Autom. ICCUBEA 2017*, pp. 1–6, 2018.
- [8] P. V. R. Murthy and R. G. Shilpa, "Vulnerability Coverage Criteria for Security Testing of Web Applications *," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 489–494, 2018.
 - [9] R. M. Parizi, K. Qian, H. Shahriar, F. Wu, and L. Tao, "Benchmark Requirements for Assessing Software Security Vulnerability Testing Tools," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, pp. 825–826, 2018.
 - [10] "Vulnerability Assessment and Penetration Testing through Artificial Intelligence," *Int. J. Recent Trends Eng. Res.*, vol. 4, no. 1, pp. 217–224, 2018.
 - [11] "VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)," *Int. J. Recent Trends Eng. Res.*, vol. 4, no. 3, pp. 326–330, 2018.
 - [12] P. Description, "Cyber Security Awareness , Behaviour and Culture Analysis , Training and Risk Mitigation."
 - [13] O. N. E. Click and C. A. N. Change, "s a w n o i t a t u p My re s u o i c i l a m y b ruined."
 - [14] R. J. Ray, "Training Programs to Increase Cybersecurity Awareness and Compliance in Nonprofits," vol. 1277, no. December 2014, 2014.
 - [15] G. Sidaway, "Security Breaches - What's the Real Cost to the Business?," *Credit Control*, vol. 38, no. 3/4, pp. 41–45, 2017.
 - [16] L. Ablon, P. Heaton, D. Lavery, and S. Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*. 2016.
 - [17] P. L. Schaffer, E. Velasquez, N. Fiorentino, K. Dwyer, A. Hamilton, and K. Barney, "GeneraliGlobalAssistance-IDP.com 2 PRESIDENT & COO, GLOBAL IDENTITY & DIGITAL PROTECTION SERVICES GENERALI GLOBAL ASSISTANCE (GGA)," 2018.
 - [18] Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 2015.
 - [19] N. B. Al Barghuthi, M. Saleh, S. Alsuwaidi, and S. Alhammadi, "Evaluation of portable penetration testing on smart cities applications using Raspberry Pi III," in *2017 Fourth HCT Information Technology Trends (ITT)*, 2017, pp. 67–72.
 - [20] H. R. H. Hamid, M. A. I. B. M. A. Kamil, and N. Y. Abdullah, "Portable Toolkit for Penetration Testing and Firewall Configuration," *Proc. - 4th Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensics, CyberSec 2015*, pp. 90–94, 2016.
 - [21] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," *2018 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2018*, pp. 1–7, 2018.

Research Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

79/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

GRADING FORM: NEW ASSESSMENT

RUMEN CHOWDHURY

79

ENGAGEMENT WITH LITERATURE



A very good discussion but would be good to critically evaluate related works. Appropriate

11

sources used.

KNOWLEDGE AND UNDERSTANDING

- 

The aim is well defined with appropriate objectives. The relevant knowledge and understanding were displayed throughout the written document and more so the research aspect. The conclusion summed up the proposal but not the expected outcomes of the alternative method to penetration testing.
- 11**

COGNITIVE, INTELLECTUAL SKILLS

- 

This was clearly highlighted and explained. All tools needed were listed as well
- 13**

PRACTICAL SKILLS

- 

The appropriate methods were discuss and aligned to the project. Timeline with resources done a graphical Gantt chart would be good. Ethics form completed.
- 36**

TRANSFERABLE SKILLS

- 

Well presented, written and flow.
- 8**