

Irfan Onur

by Irfan Onur

FILE	2778_IRFAN_ONUR_IRFAN_ONUR_93935_186882118.DOCX (271.1K)		
TIME SUBMITTED	08-MAY-2019 11:33PM (UTC+0100)	WORD COUNT	7331
SUBMISSION ID	106705175	CHARACTER COUNT	41227



Penetration Testing of Home & Industrial Networks

MSc Computer Networks & Cyber security



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Irfan Onur (P147861)

UNIVERSITY OF WALES TRINITY SAINT DAVID School Of Applied Computing

Abstract

This document is produced to find potential exploits and solutions within the home and industrial networks that are used within daily varying from logical and physical devices. The author is set to produce a successful penetration test for a home and educational institution live network. Once potential vulnerabilities are dedicated and identified the author is obligated to find potential solutions to ensure maximized security and that every known vulnerability is secured. The author performs several types of penetration testing of the proposed networks using different methodologies and methods such as finding vulnerabilities all findings does not need to only be a part of the network equipment, but any device connected to the network topology. Devices that may also be connected to the network may be vulnerable devices such as IoT (Internet of Things) devices and other logical and physical devices. The project will be based on the intention of producing a more successful network this can vary from ensuring better communicational configurations and advanced security which will ensure encrypted end-to-end encryption and improved network topology. The proposed solutions will be submitted to the network administrator to be approved to ensure that it will be suitable to be implemented and will not be the cause of any failures or clusters.

Table of Contents

ABSTRACT.....	2
INTRODUCTION	4
AIMS & OBJECTIVES	5
AIM	5
OBJECTIVES:	5
BACKGROUND AND LITERATURE RESEARCH.....	6
CURRENT LITERATURE & BACKGROUND RESEARCH	6
<i>Previous threats and breaches of industrial network</i>	<i>6</i>
<i>Network protocols & current security features of common industrial networks</i>	<i>7</i>
<i>Impacts of Cybersecurity Breaches</i>	<i>7</i>
LITERATURE REVIEW.....	8
<i>Development of penetration testing model for increasing network security.....</i>	<i>8</i>
<i>Research of behaviour-based penetration testing model of the network</i>	<i>9</i>
<i>Testing of penetration testing process and tools.....</i>	<i>10</i>
<i>Similar areas of focus.....</i>	<i>11</i>
RESEARCH METHODS.....	12
PHILOSOPHY	12
STRATEGY'S	13
APPROACHES	14
<i>Experiment.....</i>	<i>14</i>
<i>Action Research.....</i>	<i>14</i>
<i>Grounded Theory.....</i>	<i>14</i>
RISKS & LIMITATIONS	14
DATA EVALUATION.....	15
RESOURCE & PLANNING.....	16
REQUIRED RESOURCES	16
PLANNING OF A PENETRATION TESTING	17
GANTT CHART	18
ETHICAL CONSIDERATIONS.....	19
BENEFITS OF THE PROJECT	20
DISADVANTAGES OF PROJECT.....	21
DISASTER RECOVERY	21
CONCLUSION	22
REFERENCES	23
TABLE OF FIGURES.....	25

Introduction

This document was produced to perform various security penetration testing using techniques based on black and grey box penetration testing. The various tools and methods used to perform a penetration test will be based on a standard home network and an educational live network. The proposed education institution that will participate will be the University of Wales Trinity Saint David (UWTSD), Swansea IQ campus[1]. The initial testing will be based on black box penetration testing which revokes the author or hacker to have obtained any knowledge on specs or gathering of information on the tested network, once a complete black box penetration test had been performed the hacker will have obtained some information based on the network to potentially obtain additional exploitation information to use and gather potential solution's to be implemented for the safeguarding of the network. The author will be required to perform a test with operational real-time networks and will need to ensure the integrity of data and to also ensure no disruption to the network.

Secondly, the proposed penetration test is to be tested to its highest confidentiality with strict logging of information to ensure protecting personal information as any test might leave the network to further vulnerabilities, successful tests will justify full access to the author to access personal information with registered members of the network. Registered users will be the people connected to the network including Staff, Student and Guest. Connection to educational networks requires certain personal data for the connected users, these sorts of data are protected via term and conditions this requires institutions to enforce maximized security for data relating to personal data acts and regulations set by cyber laws. These laws are protected by acts of the Great Britain act of the parliament, which is to defend personal data that will be registered on record either on physical or electronic storage within any organization this act was enforced in power in the year of 1998[2].

Public, Private, Government or any other type of organization that requires to collect data or which requires to store data on personal or confidential information is enforced by law to ensure strict security to protect the data or will be criminally prosecuted. Educational institution requires constant network protection and monitoring as they require to store confidential or personal information such as Banking, Medical reports, Identity and etc. unethical hackers that gain access can cause massive chaos as they will use stolen data to either blackmail the institution or use their findings to support or proceed within further criminal activity. The author will report any findings even if they were either successful or failed to ensure the integrity of the testing as the institution can be aware of additional threats that could have not been protected by the author. This documentation is to ensure understanding and extensive knowledge of security systems, penetration testing and advanced security implementations.

Aims & Objectives

Aim

Black box penetration testing to assess the security exploits and potential vulnerabilities of a network and propose solutions to any vulnerabilities that may be found within the network.

Objectives:

- Improved learning area's
- Research and literature review
- Vulnerability assessment and penetration testing of home/industrial networks
- Vulnerability assessment towards an IoT device and home/industrial network to exploit the integrity
- Write the work up in good form with appropriate detailed research
- Vulnerability assessment to discover potential security threats
- Use findings to perform ethical breach into a network to support the hypothesis of the finding
- Produce a security solution
- Ensure provided network for university members (Staff/Students) is at maximised security to ensure safety for users
- Final Outcome

Background and literature Research

This chapter will be broken to two subchapters, the first sub-chapter will discuss gathered information based on security exploits that had unethically been tested and been neutralized as soon as it had been discovered by the proper authority. The second part of this chapter will be research papers aiding the author in knowledge and key skill to ensure a successful penetration test with potential and successful solutions.

Current Literature & Background research

Previous threats and breaches of industrial network

The author will initially propose penetration testing to the University of Wales Trinity Saint David's industrial network, and which will discuss networks attacks at previous dates some of these attacks were performed by black hat hackers and some attacks had potentially been for educational use by cybersecurity students, Dates and attacks are documented below:

- The academic year 2014-2015, Network port attack (infinite network loop)
- The academic year 2016-2017, Virus/Malware Based attack
- The academic year 2017-2018, DDoS based attack
- The academic year 2018-2019, Network Login cracker

The university was enforced to execute certain strategies and actions to perform safety of network and security solutions of any similar types of vulnerabilities that were used to attack the network. The university is required by law to produce quick risk assessments and vulnerability solutions to ensure further attacks or to keep live attacks damage to a minimum this meaning to ensure quick and secure proceeding to be implemented immediately.

Cost:

- The university was forced to add extra paid staff hours when previous attacks were in process to obtain control and safety of the network
- The university had previously obtained additional resources and security consultants to ensure maximized security
- Additional employee hours can occur with overtime pay
- External resources will be required such as third-party companies, lawful authorities, security consultants

Potential Risk:

- When an educational institution is attacked this may compromise confidential information such as personal details, Financial details and etc.
- Loss of Data
- Compromised information
- Criminal prosecutions / lawful prosecution

Post-attack Effects:

- Network disruption
- Students affected by network affects the studies of students
- Data Loss (Educational findings, Research papers, Educational & etc)
- Cost

Network protocols & current security features of common industrial networks

Current educational institutions all operate within Wi-Fi mesh network[3], [4] throughout an entire physical location with multiple access points (AP) based in indoor and outdoor environment's[5], [6] to allow access to the internet, intranet and extranet, the use of the AP's allow all registered members access to the network.

In the United Kingdom, all academic institution is entirely connected use the same backbone intranet network, which is known as the JANET Network[7]–[10] (Joint Academic Network), there is also an improved and advanced version of the Backbone network known as Super JANET but is currently not utilised within every academic institution this is due to networks which are not updated, old operating systems and configurations, poorly protected networks.

Impacts of Cybersecurity Breaches

Within the past years, there have been several encounters of cybersecurity breaches that have impacted many organizations which the cause of huge exposure for data has been, money and etc. Cisco has estimated that there will be 500 billion IoT (Internet of Things) devices to be connected to the internet by 2030 and IoT has already shown an increase of 600% in 2017[11].

Research indicates that 74% of companies have over 1,000 stale sensitive files stolen[12], 21% of all files are not protected with any type of security feature. Most attacks are based within spear-emails which current estimation proves 71%[13]. In the year 2017 virus attacks were increased to a total of 5.4 billion attacks. It cost many companies \$2.4 billion in malware attacks which is also an increase of 22.7% from 2016 to 2017[14]. The average cost for security intrusion was an average of \$11.7 million in 2017[15] which was also not protected using up-to-date security features with one of the factors including penetration testing.

Literature Review

The author also searches through other case studies to try finding vulnerabilities, disadvantages and advantages. This allows the authors to improve their own project without making it more complicated. While the writer researched many different case studies, this allowed the author to learn various different creative ideas from other researchers and developers. Some of the numerous creative ideas from different researchers are analysed and reviewed for the future development of this project.

Development of penetration testing model for increasing network security

This research was conducted to show the importance that relies on networking and penetration testing, it relates to the use of the internet being the major tool used for the exchange of information. The author of the research documents justifies that networks are very venerable to attacks as quoted “Network administrators have often tried their best by improving their network security”. The author dictates that even with growth and extensive knowledge of security, that it is still not enough to ensure the integrity of any security platform as hackers are introduced to varieties of new exploitation methods and techniques every day and with the rapid growth of black hat hackers towards white hat hackers are at the very intensive difference.

The author of the research paper suggests that “the best way of ensuring that the system is secure is to attempt penetration testing. This would be the most effective way to find exploits and to proof whether a system is vulnerable[16]”. The research document supports the hypothesis of the author of the proposal in the suggestion that security platforms require constant validations and regular penetration testing to ensure the integrity of IT/Network infrastructures. As indicated penetration testing is a real-world scenario confirmation of vulnerable exploitation’s and thereby allows a birds-eye perspective on current security.

The document researched shows relevance and importance that penetration testing produces information and data based on exposure this can relate publicly to the network or through the internet which is justified “proof of concept”, the author obtains knowledge through the research conference proceeding that different vectors of security requires additional hours of study and focus to ensure that every effort has been made to study the extensive knowledge of protocol or vulnerability.

Information gathered shows that ideas and knowledge of professionals within IT and cybersecurity professionals’ input and suggestions should all be put in practice to show a greater knowledge of understanding and extensive knowledge on security systems to protect further solutions. professionals

Research of behaviour-based penetration testing model of the network

This research was conducted to support the basis of a three-tier attack which includes the preparation of the attack, the attack phase and the post-attack phase[17], this document support the basis of a prepared and planned attack to be successful as necessary knowledge and understanding would be conducted prior to the attack stated as the pre-attack.

The produced document supports the aspects of the project of ensuring that the penetration testing to be ensured without any disruptions and ensuring that all executed work will not cause any damage to the operational live network. This is by enabling the use of a pre-attack this is the definition of preparing for any potential findings such as vulnerabilities to ensuring the use and purpose of the vulnerability is clearly planned this is to enable the attacker to obtain extensive knowledge of the findings. Sometimes some protocols may need to enable but can ideally be secured via the use of encryption ensuring that it is much more difficult for an attacker to obtain access. some aspects of pre-attack are to be informed to every user of the network that there will be maintenance works on the network and that it may be unavailable at the time of the penetration testing. In the technical terminology, the pre-attack is separated into two categories which are based towards active reconnaissance and passive reconnaissance. Passive reconnaissance is where an attacker does not touch the network to gather all relevant information as possible once all relevant data is collected only when the attacker will begin an active reconnaissance.

The document is then set to show and explain the terminology of the attack phase of a penetration test which is documented to show that there are several steps to complete an attack phase of a PEN test. The attack phase is when the attacker will take every precaution step to ensure the integrity of the performed test by exploiting every vulnerability found with the use of various different tools and methods to ensure a successful test. Attackers could easily gain access to any network that operates with a weak security policy, ideally an attack phase consists of firstly penetrate perimeter of the ideal network then the attacker will need to acquire target network, after the initial first two steps the attacker will escalate the privileges to their dummy account which will ensure the execution of exploits or implant of viruses and retracts of information/data.

The final stage that is proposed from the analysed document will be the post-attack phase, is the justification and solutions of an improved more advanced/enhanced network with maximised security assurance. The attacker may also be required in some scenarios to restore the network to the pre-test state if the network administrator will not require the changes to network this may sometimes be the issue as some networks still require back-door or remote access to certain devices which may be the cause of leaving an entire network vulnerable.

In conclusion, the author suggests that the document support high knowledge in understanding the preparation and penetration testing without any exposures to unethical hackers, the document supports the advancement of PEN testing and understanding the importance on dealing with sensitive data. The author is able to execute the findings within their own submission of a successful PEN test.

Testing of penetration testing process and tools

The demonstrated paper discusses the importance of penetration testing and states that “every technological advance raises new security threat that requires new security solutions.” [18]. The findings on the research paper consist of the development and production of enchantments within networks and other areas that require security features to protect their purpose which can be aided with the management of higher security goals.

Key indicators of the paper help aid and show understanding of newer vulnerabilities are discovered within every second passing by as there are attackers looking at the methods to ensure ways to exploit them, there are different factors of hackers which are classified as black, white or grey hat hackers with consideration of ethical rights they will need to approve to ensure that lawful grounds of the law are governed also to protect sensitive exposure to data. The paper also demonstrates understanding and implementation of Information Security Management System (isms) which is designed in relation to the international standards for information security management, which is used to help aid information confidentiality, information integrity and service availability, the known model is also recognised by the Plan Do Check and Act (PDCA) model.

Other key points identified are external & internal testing, router, firewall, application, IDS, Password cracking penetration, social engineering test and the process of completing a successful test. Three phases of a penetration test process that need to be taken into consideration are preparation, implementation and analysis. Where the preparation phase will involve the scope of the system components, objective of the testing, duration and time are identified, which will be required to be agreed and documented. Other aspects also covered are like possible information leakage, potential downtime is also acknowledged and are predictable in the legal documents and are approved and authorized by both parties.

The second phase will be the scope of the implementation of the penetration testing, this will involve information gathering, vulnerability analysis and vulnerability exploits. These acquired steps will ensure the success of the test and the integrity of data exposure. Tests can also be conducted by using automated testing tools or manual testing or both simultaneously. Prior to completion of any penetration test, a suitable analysis will be required to be conducted this will also be recognized as the reporting phase.

The reporting phase is to deliver suggested and various reports to senior management through the reporting process, IT management and technical staff will all likely see some or the whole of the report. The produced report should have sections based upon essential Summary, Technical aspect, assessment Discoveries, Risk Level suggestion summary, Budget Estimation and etc... with the use of a report a pen tester is capable to represent the entire executed work to the suitable authority, so a suitable solution can be presented.

In summarization of the researched paper indicated the author is able to obtain resourceful information to progress in the completion of the aims and objectives of the project outcome, the author understands the suitable ethics and right that will need to consider to the completion of the project and suitable production of reports to conclude in the completion of any penetration test and who will be the correct authority to pass along the suitable reports.

Similar areas of focus

The author uses this part to demonstrate briefly other documents that state similar research or other aspects that need to be taken into consideration to ensure a successful outcome covering all possible areas of importance. One of many papers researched is “testing production systems safely: common precautions in penetration testing[19]” this paper indicates different strategies that can be implemented to a variety of different types of penetration test to ensure that all risk can be maintained to a minimum effect. The key summary of the paper concludes penetration testing suggests that the secondary objective of a test is not harming the target. The preparation of handling the test target as a black box, in many cases the testers propose for the sake of ‘realism’, therefore seems doubtful. Testers need to think like an unethical attacker, but they should not be in the same situation regarding prior knowledge of the target, considering any limitations is to be concluded in the production phase of the test. Other identifiers are a potential disaster and recovery options based on a business and technical scope.

Another research paper includes “automated penetration testing based on a threat model [20]” which disuses the systematic approach for penetration testing for testers with the aid of guided algorithms by a threat model. The use of a threat model is to ensure all vulnerabilities are assessed and no security breach is not overlooked through the process of testing. So the research paper backs its own hypostasis of an automated penetration testing tool kit with the use of a real-life environment to be tested upon.

The automated system produced with the use of the algorithm is tasked with seven different phases to complete which include: planning, system modelling, threats extraction using the threat model, vulnerability discovery, threat and vulnerability mapping, attack and reporting. The researcher of the proposed paper indicates this automated system is not valid for all types of platform and is only acquired for certain groups to be implemented towards. In summarization, the author believes the automated system may be a good practice to be followed for a potential daily penetration test that is run to overcome small vulnerabilities that can be found on an everyday system.

Thirdly another research paper that was briefly summarized as “penetration testing in the IoT age[21]”, the paper continuously states the rapid growth of IoT and all the new security threats that come along with it and how white hat hackers are meant to evolve their knowledge and skills to overcome security threats. The challenges stated is based upon offensive attacks and how malicious attacks may only require a single potential type of vulnerability to exploit an entire system or network. The paper indicates that pen testers should produce automated systems for specific areas of penetration testing to substitute any irrelevant testing time.

In summarization, the demonstrated paper indicates a majority of key points to help evolve the progression of the outcome of the project with the aid of encapsulation, intelligent grey-Box testing, virtual machine introspection and system testing. The paper suggests strong key information on different phases of attacks that will need to be obtained to exploit any system and why there shall be a group of specific information gathering prior to attack implementation. The paper also provides research-based upon intelligent entry-point crawling and ways to work around it as it consumes a lot of time, other indicators are newer network infrastructures with developed security features that are proposed.

Research Methods

Philosophy

Based on the research onion [22], [23] researched to help aid the understanding of the research philosophy criteria, the first layer of the research onion is based on Research Philosophy. This category focuses on three different aspects, which consist of Positivism, Realism, and Interpretivism. The author believes that the project only focuses on the aspects of Positivism and realism the author shows below how he believes how it relates to the proposed project.

- **Positivism:**

The positivism aspect within a research onion is used to generate a hypothesis of a research paper so that the scientific experiment or statistics that acquire the requirement of data collection can be tested and that the author or researcher should not have a bias opinion on the collected data. All data collected should be analyzed and conducted in scientific terminology. This implies that the author should analyze and compare the results found in previous research areas and fields to obtain the integrity of the test. This will also ensure that the author can observe and be able to describe the reality from an objective point of view.

The author implies positivism to the project by gathering research data on the background and research papers based on the project hypotheses. The author continues through the entire project by applying multiple research's in-depth within various similar areas to check current, previous and future upcoming developments in their field to compare and improve the project outcomes. All research and gathered data by the researcher were from official academic and scientific sources to only allow the use of formal and ethical researchers which have been approved from suitable authorities which help maintain the professionalism of the project.

- **Realism:**

The realism aspect known to the research onion terminology describes being used when a researcher is uncertain if the gathered information is enough to determine a fully anticipated result or outcome of the overall project to be suggested by the author. Realism uses the aspects to allow the researcher to consult with third-party people to analyze upon their own and others' opinions continuously to not create a biased result for this project the other people can be the current network administrators. Realism uses the aspect of always research to constantly research various types of research theories, as the terminology for realism states that the ability to know for certain meaning 100% so this will be what the reality it will not exist if not researched continuously, this enables the researcher's opinion to be open to newer suggest and theories by using many new methods for development of the research.

The author suggests that realism should be an approached aspect for the benefit of this research as it is believed that the improvement of cybersecurity will always require constant research as there are newer vulnerabilities discovered every day. The author suggests that due to a vulnerability within any physical and logical device there should always be updated research gathered to help improve unknown areas, which within networks there are data transmission at all times which require to obtain data this could be confidential and could be intercepted by hackers, which could leave a huge breach in information, so realism ensures latest security features.

Strategy's

- **Experiment**

This aspect ensures the author permissions to test the hypothesis to generate data to be collected and test the data, so it can be statistically analyzed.

- **Survey**

This strategy allows the author to gather various different types of data. The advantages of a survey are that all questions on the survey are set by the researcher to gather correct data surveys allows the ability to gain a non-bias opinion.

- **Case study**

This aspect ensures the author in allowing an extensive study of experiments based on objects, person or on other case studies in a real-life environment. Gathered data will require a detailed analyzation and this aspect can occur with video footage recording to assess the behaviours of the experiment.

- **Action research**

This aspect ensures the author the ability to help solve a hypothesis with the aid of different varieties of actions based on a list.

- **Grounded theory**

This aspect implies the inductive research approach method is used, this terminology ensures the production of a new theory in comparison to alternative existing theories, the related research literature is also appropriate also data gathering is suitable in aiding the production of a new theory.

- **Ethnography**

This terminology states that the researcher is to be a part of the research area, community or situation to enable the researcher to give a full in-depth description of the collected data on a day-to-day basis. This aspect is very time consuming as the integrity of the test is based on the amount of time spent.

- **Archival research**

This aspect is used to test present data that is generated against archive test results, this aspect could not always be preferred due to the sole purpose of the information integrity as it could always be vulnerable to a malicious edit which could provide false information.

Approaches

The author is obligated to select three ideal approaches to seem fit for the purpose of the outcome of the project and the development with the assurance of success. Below the author demonstrates what they have seen fit for the purpose of the project and why that method is selected for the initial use of the methodology of the project.

Experiment

This project requires various types of experiments and will require them to be supervised to ensure the integrity of the collected data. All found will be confidential data of the industrial network.

Action Research

The author will proceed with the aspect of Action Research to help conduct background and literature reviews based on past case studies and current case studies, scenarios, experiments, hypothesis and test their ability with the conducted new project.

Grounded Theory

The author will obtain knowledge and understanding of previously conducted hypothesis and in the test the collected data against the obtained data and test the comparison analysis. This will help to have a better understanding of the outcome of the project as there can be comparisons with previous successful penetration test and if there have been any improvements.

Risks & Limitations

The author is not able to ensure the integrity of the PEN test and therefore faces the chances of potential risk and limitations. Some of the identified risk at this stage of the penetration test is known to be data loss, interruption to network, network overflow which may cause the network to crash, attack from an unethical attacker which may take advantage of the ethical PEN test attack.

The identified risk may be able to be avoided if preparations and cautions are taken to ensure the integrity and sensitivity of the network, the author could set warnings and maintenance logs to ensure every change is recorded this ensures that any changes made that will cause damage to the network can be tweaked to ensure the network will not be down.

Limitations faced by the author is the understanding of computer programming language, the author is limited with the amount of knowledge and understanding of programming languages and faces the difficulty in understanding the exploited code that is shown a part of the vulnerability that will be located within the PEN test.

The author is able to perform several different types of vulnerabilities only with the knowledge of programming language which will help the author/attacker to find potential vulnerabilities in poorly written codes and software.

Data Evaluation

Data collected through the gathering process of the penetration testing will be collected sensitively as the gathered data will be protected by the acts of data protection act 1998. All gathered document will be in a suitable lab environment which will be selected via the network administrator of the proposed network that will be attacked, this is to ensure that all exposed data is not obtained or seen via others that do acquire the same credentials.

The data collection process of an analytical correspondence to the research approach decision incorporates the design overview as the correct approach for the collection of data will effort best for the appropriate proposal, which the results will be analysed accordingly to answer any hypothesis created.

Resource & Planning

Required Resources

The author/ethical attacker is required to obtain legal ethical rights by the University of Wales Trinity Saint David before starting any type of vulnerability assessment or penetration testing. If the author had been declined of any ethical rights the author will be prosecuted with criminal charges as the author will not have any access privileges and may cause the university chaos.

The use of network attacks is that an attacker could obtain all traffic to their personal device with the use of wireless or Local physical connection to monitor the data, this data could be used later by the attacker to blackmail the victim.

The author also gathers information on possible tools that may be used incorporation to perform exploitations of both the home and industrial network majority of these tools can only be used in Kali Linux Operating[24], [25] Platform:

- Sniffing and spoofing attack, these types of attacks are used to impersonate a victim device on a network it can also be used to attack a network to steal data, spread malware, bypass access controls and etc. (Port Scanning, Wireshark network monitoring[26], [27])
- Social Engineering attacks: Maltego, Backdoor[28][25], [29]
- Database assessment: sqlmap, sqldict, sqlsus, oscanner[30]
- Reverse engineering/Backdoor attack: this type of attack method is used remotely, the majority of backdoors are designed to bypass intrusion detection systems. (jad, flasm, clang++, olydbg)[31]
- Password cracking: Cewl, John, Johnny, ncrack, pyrit, rainbowcracker, crunch, hashcat[32]
- Wireless attacks: WPA/WPA-2 Attacks, fern wifi cracker, kismet, mfterm, reaver[33]
- Session hijacking/cookie hijacking: this type of attack Is used to exploit a valid device session to gain unauthorised access to information on the device.
- SSL attacks: SSL is an encryption method used on websites (example https) an SSL attack intercepts encrypted messages before they're encrypted.

Planning of a Penetration testing

The author uses this sub-section to demonstrate potential methods that can be planned carefully and executed a successful outcome, there is various ways of penetration testing that may be executed to locate and exploit potential vulnerabilities.

Below the author demonstrate potential types of experiments to ensure the outcome of successful penetration testing this is only completed by ensuring the different types of methodologies to be approached for experiments that can be complete which will be used to exploit any discovery of vulnerabilities:

- Information gathering
- Vulnerability analysis
- External penetration testing
- Internal network penetration testing
- Wireless network penetration testing
- IDS (Intrusion Detection System) penetration testing
- Firewall penetration testing
- Router penetration testing
- Denial of Service (DoS) & Distributed Denial of Service (DDoS) penetration testing
- Application penetration testing
- Database penetration testing
- VPN (Virtual Private Network) penetration testing

Gantt Chart

The author proposes an outlined Gantt chart which was produced with windows Microsoft project[34] which is to aid the date attributes of the project and to ensure time management is carefully planned to guarantee a maximized success of the outcome of aim and objectives. The author states all dates that have been provided to them such as start and end dates, the author also dictates the proposal factors of the project such as class presentation and poster.

		Task Mode ▾	Task Name ▾	Duration ▾	Start ▾	Finish ▾	Predecessors ▾
1			Major Project	171 days	Mon 07/01/19	Mon 02/09/19	
2			Propasal	11 days	Mon 07/01/19	Mon 21/01/19	
3			poster	10 days	Tue 22/01/19	Mon 04/02/19	2
4			presentatio	18 days	Tue 05/02/19	Thu 28/02/19	3
5			Chapter 1 - Introduction	7 days	Fri 03/05/19	Mon 13/05/19	4
6			Chapter 2 - Literature & Background Research	23 days	Tue 14/05/19	Thu 13/06/19	5
7			Chapter 3 - Research	12 days	Fri 14/06/19	Mon 01/07/19	6
8			Chapter 4 - Plannin	6 days	Tue 02/07/19	Tue 09/07/19	7
9			chapter 5 - Implementation	12 days	Wed 10/07/19	Thu 25/07/19	8
10			Chapter 6 - Testing	12 days	Fri 26/07/19	Mon 12/08/19	9
11			Chapter 7 - Analysis of results	6 days	Tue 13/08/19	Tue 20/08/19	10
12			chapter 8 - conclusions	4 days	Wed 21/08/19	Mon 26/08/19	11
13			chapter 9 - references	1 day	Tue 27/08/19	Tue 27/08/19	12
14			Chapter 10 - Refelections	3 days	Wed 28/08/19	Fri 30/08/19	13

Figure 1 - Gantt Chart

A completed an updated version of the Gantt chart will be implemented to the final project paper to show a comparison of the first proposed work and the final submission to show what was initially expected of the outcome of the project and what had initially been done.

Ethical considerations

The author will be required to obtain several types of ethical rights and declaration due to sensitive data exposure, if they will be successful within breaching into a network, organisations require external parties to obtain legal rights to access restricted data and the types of rights and signatures that will be required to completing the outcome goals of this project are:

- Ethical rights of the Data Protection Act 1998[2]
- Computer Misuse Act 1990[35]
- BCS (British Computer Society) [36]
- Declaration of secrecy 1970[37]
- IEEE (Institution of Electrical & Electronic Engineering), 2010[38]
- IEEE computer society (IEEE CS)[39]
- BCS – The chartered institute for IT, 2010[40]
- BCS Information Security Specialist Group BCS-ISSG[40]
- Official Secrets Act 1989 [41]
- Equability act 2010[42]
- General data protection regulation 2018[43]
- Institute of information security professionals (iisp) [44]

Benefits of the project

The solution's that have an immediate effect with up-to-date security updates and newer security features which can be proposed with the outcome of a successful penetration test:

- Fully operational and secure network
- Fewer or no security risk
- Lower cost
- Advanced security
- Ensuring no loss of data

There are more than several benefits of the proposed project as it ensures to potentials of an encrypted network which will provide end-to-end encrypted connectivity with end devices and network devices. The final step of the project will be to ensure an advanced and improved network.

Disadvantages of project

The proposed project also might occur with some disadvantages as does many any experiment, any sort of experiment is required to ensure reports and analysis to ensure the integrity and vulnerability of the experiment. After thorough research is conducted to determine potential possible disaster scenarios and how they can be recovery options the author is able to obtain an initial understanding of possible disasters scenarios and how to overcome them.

The author is likely to have three initial disaster scenarios but if the penetration testing is conducted with 100% caution these disasters may be able to be avoided. The three identified potential disasters are the disruption of network traffic, loss of network connectivity and potential alternative vulnerabilities (sometimes penetration testers leave open ports by accident which can cause further vulnerabilities).

All potential vulnerabilities can be avoided using a clearly planned preparation for a successful outcome of the penetration test to be performed on the university live network. Every test should also be supervised to avoid any suspension of breach of ethics as the author would be able to access all sort of sensitive data.

Disaster Recovery

The author proposes several factors of disaster recovery scenarios to ensure safety measures are met in any case of a failed penetration test which might lead to a network failure. Disaster scenarios can occur from many various reasons such as incorrectly gathered information, bandwidth overflow, faulty network and etc which can be the cause of loss of data, server failure, network failure.

To ensure those disaster scenarios are carefully discussed and taken into considerations actions should also be prepared to be taken in place to allow users of the network no disruption and a fully operational network that can be accessed internally and remotely.

Planning of disaster scenarios can involve factors such as primary and secondary back-ups of both network and storage to ensure no data loss, other methods that can be implemented is system image cloning. Other methods can involve raid 5 storage disk cloning which can also be used for network configurations including the wireless spectrum.

Conclusion

The author believes that in the final outcome of the project there will be a lot of evidence to show the importance of penetration testing and the implementation of up-to-date security features, software and tools. Factors of the project initiate interesting factors to persuade security and the effects which will help the understanding of the importance of penetration testing within the home and industrial networks.

The author will demonstrate great understanding, knowledge, skills, research and experiments throughout the timescale of the project to ensure its integrity of a successful outcome by initiating disaster recovery scenarios and other methodologies of aspect to execute in case of failed penetration testing.

Completion of information gathering and vulnerability assessment was executed the author completes reports to indicate the understanding of collected data and to execute suitable penetration test towards all discovered vulnerabilities and to also ensure the test will not disrupt the network within any sort way like as speed, availability, storage and etc.

The final aspect of the project will issue a solution that can be implemented to offer extensive security to operational networks and potential IoT devices to ensure their safety, the author will also analyse all gathered vulnerabilities and solutions implemented to show a data analysis of changes that had occurred and the statistical difference of how and why the difference affects networks.

References

- [1] T. Saint David, "UWTSD SA1," 2019. [Online]. Available: <https://www.uwtsd.ac.uk/sa1/>.
- [2] "Lawful ground," *data protection act*, 1998. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1998/29/contents>.
- [3] Tzu-Jane Tsai, Hsueh-Wen Tseng, and Ai-Chun Pang, "A new MAC protocol for Wi-Fi mesh networks," in *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA '06)*, 2006, pp. 6 pp. – 366.
- [4] A. Sumarudin and T. Adiono, "The design of high throughput Wi-Fi mesh networked wireless sensor network using OLSR protocol," in *2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT)*, 2015, pp. 192–195.
- [5] H. Zhang, Y. Wang, X. Qiu, W. Li, and Q. Zhong, "Network operation simulation platform for network virtualization environment," in *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2015, pp. 400–403.
- [6] J. Wang and X. Liu, "Computer network security of university and preventive strategy," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, pp. 143–145.
- [7] G. L. Davis, S. Gladys, G. Lang, L. Luke, and M. Taylor, "The Canadian JANET System," *Proc. IRE*, vol. 45, no. 12, pp. 1666–1678, 1957.
- [8] L. Campbell and C. Hines, "Bandwidth Considerations in a JANET System," *Proc. IRE*, vol. 45, no. 12, pp. 1658–1660, 1957.
- [9] J. R. Dianda, "Indoor Wireless Service Signal Distribution via Broadband," in *2006 International Conference on Communication Technology*, 2006, pp. 1–3.
- [10] F. Bergenti, A. Poggi, and M. Somacher, "JaNeT: a framework for flexible Web-content retrieval," in *2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532)*, vol. 1, pp. 137–140.
- [11] "Cisco IoT Solutions | Internet of Things Services - Cisco." [Online]. Available: https://www.cisco.com/c/en_uk/solutions/internet-of-things/overview.html#~stickynav=2. [Accessed: 08-May-2019].
- [12] "full-text."
- [13] "80 Eye-Opening Cyber Security Statistics for 2019 - Hashed Out by The SSL Store™." [Online]. Available: <https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/>. [Accessed: 08-May-2019].
- [14] Accenture, "COST OF CYBER CRIME STUDY 2017 INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE Independently conducted by Ponemon Institute LLC and jointly developed by Accenture," 2017.
- [15] "Cyber attacks cost U.S. enterprises \$1.3 million on average in 2017 | CSO Online."
- [16] R. Budiarto, S. Ramadass, A. Samsudin, and S. Noor, "Development of penetration testing model for increasing network security," in *Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.*, pp. 563–564.
- [17] W. LanFang and K. HaiZhou, "A Research of Behavior-Based Penetration Testing Model of the Network," in *2012 International Conference on Industrial Control and Electronics Engineering*, 2012, pp. 1680–1683.
- [18] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2018, pp. 1–7.

- [19] S. Türpe and J. Eichler, "Testing Production Systems Safely: Common Precautions in Penetration Testing," in *2009 Testing: Academic and Industrial Conference - Practice and Research Techniques*, 2009, pp. 205–209.
- [20] N. A. Almubairik and G. Wills, "Automated penetration testing based on a threat model," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 413–414.
- [21] C.-K. Chen, Z.-K. Zhang, S.-H. Lee, and S. Shieh, "Penetration Testing in the IoT Age," *Computer (Long Beach, Calif.)*, vol. 51, no. 4, pp. 82–85, Apr. 2018.
- [22] "Research Onion."
- [23] "Outside of the Onion."
- [24] "Linux." [Online]. Available: <https://www.kali.org/>.
- [25] "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution." [Online]. Available: <https://www.kali.org/>. [Accessed: 08-May-2019].
- [26] M. Tool, "Wireshark."
- [27] "Wireshark · Go Deep." [Online]. Available: <https://www.wireshark.org/>. [Accessed: 08-May-2019].
- [28] D. Lestari, I. D. Wahyono, and I. Fadlika, "IoT based Electrical Energy Consumption Monitoring System Prototype: Case study in G4 Building Universitas Negeri Malang," in *2017 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2017, pp. 342–347.
- [29] "Paterva Home." [Online]. Available: <https://www.paterva.com/web7/>. [Accessed: 08-May-2019].
- [30] "sqlmap: automatic SQL injection and database takeover tool." [Online]. Available: <http://sqlmap.org/>. [Accessed: 08-May-2019].
- [31] "Clang - C++17, C++14, C++11 and C++98 Status." [Online]. Available: https://clang.llvm.org/cxx_status.html. [Accessed: 08-May-2019].
- [32] "CeWL | Penetration Testing Tools." [Online]. Available: <https://tools.kali.org/password-attacks/cewl>. [Accessed: 08-May-2019].
- [33] "Fern Wifi Cracker | Penetration Testing Tools." [Online]. Available: <https://tools.kali.org/wireless-attacks/fern-wifi-cracker>. [Accessed: 08-May-2019].
- [34] "Microsoft Project | Portfolio, resource & project management." [Online]. Available: <https://products.office.com/en-gb/project/project-and-portfolio-management-software>. [Accessed: 08-May-2019].
- [35] "Computer Misuse Act 1990."
- [36] "The British Computer Society (BCS) and the Code of Conduct." [Online]. Available: https://medium.com/@dadu_64294/the-british-computer-society-bcs-and-the-code-of-conduct-4efa47105a16. [Accessed: 08-May-2019].
- [37] "Taxes Management Act 1970."
- [38] "IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity." [Online]. Available: <https://www.ieee.org/>. [Accessed: 08-May-2019].
- [39] D. E. O'Leary, "Artificial Intelligence and Big Data," *IEEE Intell. Syst.*, vol. 28, no. 2, pp. 96–99, Mar. 2013.
- [40] "Information Security Specialist Group | Specialist Groups | Member groups | Membership | BCS - The Chartered Institute for IT." [Online]. Available: <https://www.bcs.org/category/19042>. [Accessed: 08-May-2019].
- [41] "Official Secrets Act 1989."
- [42] "Equality Act 2010: guidance - GOV.UK." [Online]. Available: <https://www.gov.uk/guidance/equality-act-2010-guidance>. [Accessed: 08-May-2019].
- [43] "Guide to the General Data Protection Regulation - GOV.UK." [Online]. Available:

<https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>. [Accessed: 08-May-2019].

[44] “Home.” [Online]. Available: <https://www.iisp.org/>. [Accessed: 08-May-2019].

Table of figures

FIGURE 1 - GANTT CHART	18
------------------------------	----

FINAL GRADE

GENERAL COMMENTS

Instructor

83/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

GRADING FORM: NEW ASSESSMENT

IRFAN ONUR

83

ENGAGEMENT WITH LITERATURE



An excellent lit review and discussion of related work with appropriate sources.

13

KNOWLEDGE AND UNDERSTANDING



An appropriate title for the project. The aim is well defined but the objectives could be rephrased to read better and sound like objectives. Some of them are not really objectives. Displayed excellent knowledge and understanding of Penetration testing. The conclusion summed up what the expected outcomes should be after carrying out the

11

black box penetration testing.

COGNITIVE, INTELLECTUAL SKILLS



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

14

PRACTICAL SKILLS



There were no need to include the methods that were not needed for the project. The appropriate ones were discuss and aligned to the project. Clear Gantt chart. Ethics form completed.

38

TRANSFERABLE SKILLS



Correct use of referencing. Some areas could be better written. A presentable work.

7