

Project Proposal_Daniel Carlson_2001079

by Daniel Carlson

Submission date: 20-Oct-2022 12:56PM (UTC+0100)

Submission ID: 187128300

File name: 24800_Daniel_Carlson_Project_Proposal_Daniel_Carlson_2001079_443262_2069547185.docx
(193.73K)

Word count: 2221

Character count: 12501

The Investigation, Implementation and
Mitigation of the Most Currently Used
Cyber Attacks

Research Proposal

Daniel Carlson – (Computer Networks and
Cybersecurity)

Dr Nitheesh Murugan Kaliyamurthy

17/10/2022

Table of Contents

Table of Figures.....	3
Table of Tables.....	3
1. Introduction	4
2. Background to the Proposed Research.....	5
3. Aims & Objectives	6
Aim.....	6
Objectives:	6
4. Project Design	6
4.1 Outline of Project Process.....	6
4.2 Data Collection.....	6
4.3 Data Evaluation	6
4.4 Risks & Limitations	6
4.5 Ethical Issues.....	6
5. Resources & Planning.....	7
5.1 Resources Required	7
5.1.1 Hardware Resources	7
5.1.2 Software Resources	7
5.1.3 Other Resources.....	7
5.2 Planning Chart.....	7
6. Reference List.....	8
7. Bibliography	9

Table of Figures

No table of figures entries found.

Table of Tables

No table of figures entries found.

1. Introduction

The continuous technological development in our day and age has allowed numerous breakthroughs in Cyber Security and Defence to take place, but even with development within the Security sector, there will always be some workarounds and backdoors which can be exploited and used against us, otherwise known as a cyber-attack. Since the worldwide Pandemic event occurred, the threat of data breaches and exploits has increased significantly with the development of vaccines. The use of this information has led numerous methods of vulnerabilities to come to light, such as Social Engineering and Phishing exploits.

A recent paper within the health industry has discussed and disclosed that many different healthcare providers and academic institutions have been the subject of coordinated and sophisticated cyberattacks since the outbreak started. As more cybercriminals attempt to take advantage of the weaknesses in the healthcare sector during COVID-19, both national and international federal bodies have stressed the critical necessity for healthcare providers and universities to safeguard themselves against cyberattacks. A desire to steal information about COVID-19 vaccine development, modelling, and experimental therapies, is included in this. [1]

With so much continuous development within our cyber world, there will always be an increase in threats and vulnerabilities. A research paper [2] within the investigation of vulnerabilities and threats states and identifies that Cybercriminal activity has increased exponentially because of the exponential growth in cyberspace usage. The primary cause of this growth is the overreliance on Web apps in virtually every aspect of life. These Web apps have some design flaws, and hackers take advantage of those flaws to access systems unauthorisedly.

While many papers [3], [4] are actively researching methods for counteracting these issues, not many reports show in detail how these breaches occur and how it is best to help avoid and mitigate the problems. This paper aims to investigate the most used issues and exploits currently being used to cause harm and damage to all sectors but also seeks to show the implementation of these attacks on systems and physical and software-based mitigation strategies. It is hoped that the outcome of this research paper will make its readers more aware of the exploits being used and will be a clear representation of the mitigation strategies available for use to avoid any significant destruction and loss from Cyber-attacks and Exploits.

2. Background to the Proposed Research

Within the Cyber Security Industry, there are numerous different sectors and areas to cover, but the most fundamental areas are data protection, attack mitigation and overall digital security. Untawale clearly states that "Network safety accepts a basic job in the space of information innovation. Defending the information have become the best trouble in the current day." [5] The constant use and creation of data within everything we do has now become second nature to all mankind but without thinking of all the risks it poses to create and store data without the proper measures, it can lead to numerous breaches and exploits being used by "Cyber-Criminals" to gain the upper hand on a specific organisation.

Cybercrime, which can include everything from electronic cracking to denial-of-service attacks, is a word used to generally define criminal conduct in which computers or computer networks are a tool, a target, or a venue of illegal activity. Cyber Exploits have the power to stop any railway in its tracks, lead planes in the incorrect directions while they are in flight and give other nations access to vital military information. [6] With the increasing amount of cybercrime, the methods used by these criminals are only being analysed [7] and beginning the process of mitigation, it is uncommon to see any safe methods of dealing with these criminals without first Our digital security is beginning to falter with continuous types of malware and other significant exploits. Without a proper understanding of these issues and their relevant mitigation strategies, we will soon be in a predicament where all our personal data will be freely available worldwide. Without

understanding how these specific exploits work and their effect on the targeted entity.

There are several methods that cyber-criminals use to exploit systems/organisations, it can range from being an e-mail to a physical breach. Any device that can connect to the Internet is vulnerable to a breach and/or exploitation. Attacks such as Phishing and Social Engineering [8] are currently the most used by the Cyber-Criminals to gain access to personal accounts and data. Through some dangerous links or scam emails, the user falls for the trap and gives the information. It causes the user to lose a lot of personal information, which can result in identity theft and other disastrous outcomes. Phishing attacks are currently the most significant danger to internet security and cost businesses money each year. More than half of all cybercrimes that target real users are phishing assaults. [9] But the other half of crimes are categorised into numerous other possible exploits, mainly named malware.

As commented in [10]:

The expression "malware" envelops different kinds of assaults including spyware, infections, and worms. Malware utilizes a weakness to break an organization at the point when a client clicks a "planted" risky connection or email attachment which is utilized in programming inside the framework."

further study into the implementation of these exploits, the current mitigation strategies available will soon become obsolete, and then all data will become vulnerable. The need for constant review and updates to the relevant mitigation strategies is needed to protect our cyber civilisation.

3. Aims & Objectives

Aim

Investigate common cyber-exploits on network systems to provide a greater understanding of how to identify these threats and relevant mitigating strategies to these exploits.

Objectives:

- To critically evaluate information available about common cyber exploits.
- To research available tools to demonstrate implementations.
- Using collected information, demonstrate implementation of these exploits using available tools.
- To show mitigating strategies to counteract these exploits.

4. Project Design

4.1 Outline of Project Process

Everyone at some point experiences a cyber-attack in some form whether by email (phishing), or by a chat room, it can happen at any point in your life. This has prompted me from personal experience of being subject to an exploit to research and learn to detect and mitigate from future attacks. They can range from being intentional – knowingly visiting dangerous sites and the dark web, or unintentional – accessing and activating a link within chat rooms and/or emails.

4.2 Data Collection

To use and research a variety of Simulation tools and use of peer-reviewed articles and books, research papers etc. in order to collect

data relevant to the specific objective and project area. Some relevant data collected will be about the used simulation tools used for relevant implementation and mitigation properties of the project.

4.3 Data Evaluation

To analyse data collected with available moderation methods and validity methods in order to show it is reliable. The use of multiple sources of data in order to investigate all relevant information in all articles etc. collected and the investigation of all safe to use and widely used simulation tools in order to ensure proper simulation accuracy.

4.4 Risks & Limitations

There are no severe risks or limitations to this project. There is a very minimal risk of data loss on personal devices if the proper virtual machines are not used, but these risks are very minimal and can be mitigated entirely by using caution and the proper procedure. There is a slight limitation into the specifications required to run the simulation tools, but most systems can run the tools.

4.5 Ethical Issues

There are no ethical issues within this project as all the simulations and implementations will be done on a self-created virtual machine and no personal or confidential data will be collected or stored. The only social interaction of this project will be anonymous collection of data, all other aspects will be done independently using a virtual system.

5. Resources & Planning

5.1 Resources Required

There are not many resources required within this project as most will be software based without the need for significant hardware requirements.

5.1.1 Hardware Resources

The only hardware resources needed will be a desktop or device that has the capability to run Oracle VirtualBox or VMware for use in the project. There are no other hardware requirements needed apart from those listed above.

5.1.2 Software Resources

There are numerous different software’s needed within this project. The first is a Virtual Machine software needed for implementation demonstration purposes. The two most common software available are

either Oracle VirtualBox or VMware. The use of the software Packet Tracer will also be needed as this will be required for network demonstration purposes.

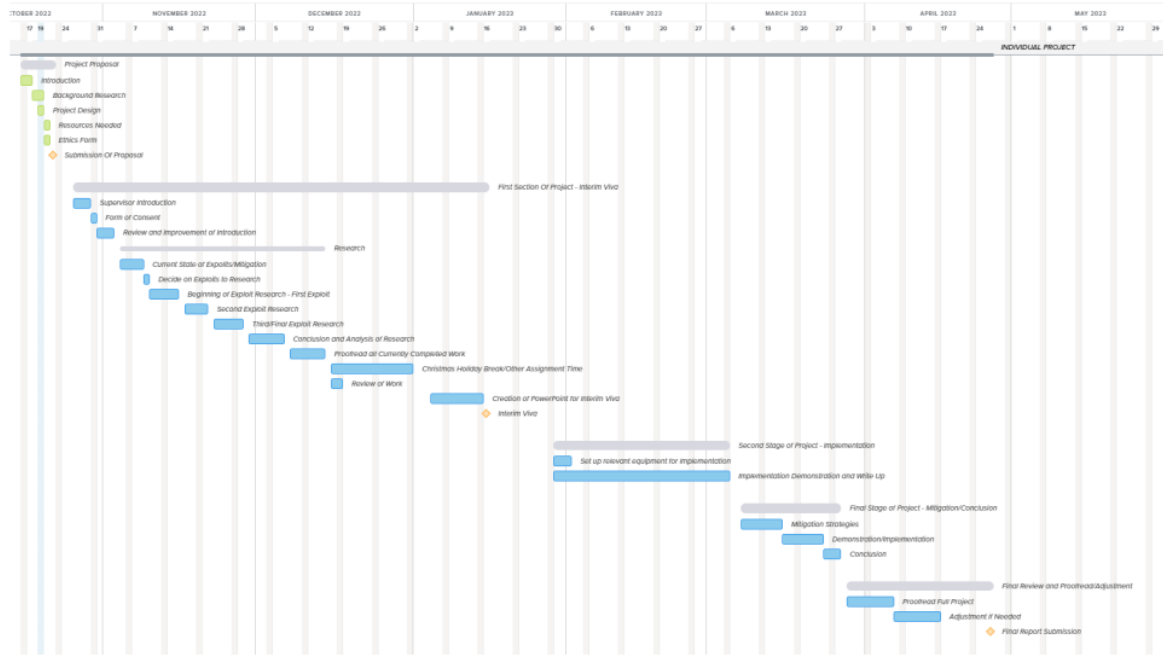
The use of necessary toolkits will be needed in order to simulate specific exploits such as the Social Engineering Toolkit which all come installed pre-installed on the Kali Linux Virtual Machine.

5.1.3 Other Resources

The final resources needed will be access to the Kali Linux Operating System as well as a licence key and download link for the Windows 10 Operating System. These will be essential in order to run specific implementations within the virtual environment.

5.2 Planning Chart

Below is a relevant Time chart which will give good deadlines and personal progression in order to complete specific areas of the project:



6. Reference List

- [1] M. Muthuppalaniappan and K. Stevenson, 'Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health', *International Journal for Quality in Health Care*, vol. 33, no. 1, 2021, doi: 10.1093/intqhc/mzaa117.
- [2] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, 'Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study', *Arab J Sci Eng*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020, doi: 10.1007/s13369-019-04319-2.
- [3] A. Chowdhury, 'Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview', in *Applications and Techniques in Information Security*, 2016, pp. 54–65.
- [4] A. Mpatziakas, S. Papadopoulos, A. Drosou, and D. Tzovaras, 'A Hypothesis Testing tool for the comparison of different Cyber-Security Mitigation Strategies in IoT'.
- [5] Prof. Ms. T. Untawale, 'Importance of Cyber Security in Digital Era', *Int J Res Appl Sci Eng Technol*, vol. 9, no. 8, pp. 963–966, Aug. 2021, doi: 10.22214/ijraset.2021.37519.
- [6] A. Professor, 'Impact of Cyber Crime: Issues and Challenges', 2019. [Online]. Available: <http://creativecommons.org/licenses/by/4.0>
- [7] A. Rawal, 'Study of Security Breaches in Internet-Cyber Crime', *International Journal of Research and Analytical Reviews*, 2019, [Online]. Available: www.ijrar.org
- [8] GCHQ and Cert-UK, 'Common Cyber Attacks: Reducing The Impact', 2020. [Online]. Available: www.gov.uk/government/publications/cyber-essentials-scheme-overview
- [9] A. K. Jain and B. B. Gupta, 'A survey of phishing attack techniques, defence mechanisms and open research challenges', *Enterprise Information Systems*, vol. 16, no. 4. Taylor and Francis Ltd., pp. 527–565, 2022. doi: 10.1080/17517575.2021.1896786.
- [10] Mr Pradeep Nayak, Mohammed Sufiyan, Monisha N S, Moolly Gautami Bhaskar, and Mohan Raju, 'Review Paper on Cyber Security and Types of Cyber Attacks', *International Journal of Advanced Research in Science, Communication and Technology*, pp. 732–735, Aug. 2022, doi: 10.48175/ijarsct-7043.

7. Bibliography

- [1] M. Muthuppalaniappan and K. Stevenson, 'Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health', *International Journal for Quality in Health Care*, vol. 33, no. 1, 2021, doi: 10.1093/intqhc/mzaa117.
- [2] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, 'Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study', *Arab J Sci Eng*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020, doi: 10.1007/s13369-019-04319-2.
- [3] A. Chowdhury, 'Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview', in *Applications and Techniques in Information Security*, 2016, pp. 54–65.
- [4] A. Mpatziakas, S. Papadopoulos, A. Drosou, and D. Tzovaras, 'A Hypothesis Testing tool for the comparison of different Cyber-Security Mitigation Strategies in IoT'.
- [5] Prof. Ms. T. Untawale, 'Importance of Cyber Security in Digital Era', *Int J Res Appl Sci Eng Technol*, vol. 9, no. 8, pp. 963–966, Aug. 2021, doi: 10.22214/ijraset.2021.37519.
- [6] A. Professor, 'Impact of Cyber Crime: Issues and Challenges', 2019. [Online]. Available: <http://creativecommons.org/licenses/by/4.0>
- [7] A. Rawal, 'Study of Security Breaches in Internet-Cyber Crime', *International Journal of Research and Analytical Reviews*, 2019, [Online]. Available: www.ijrar.org
- [8] GCHQ and Cert-UK, 'Common Cyber Attacks: Reducing The Impact', 2020. [Online]. Available: www.gov.uk/government/publications/cyber-essentials-scheme-overview
- [9] A. K. Jain and B. B. Gupta, 'A survey of phishing attack techniques, defence mechanisms and open research challenges', *Enterprise Information Systems*, vol. 16, no. 4. Taylor and Francis Ltd., pp. 527–565, 2022. doi: 10.1080/17517575.2021.1896786.
- [10] Mr Pradeep Nayak, Mohammed Sufiyan, Monisha N S, Moolly Gautami Bhaskar, and Mohan Raju, 'Review Paper on Cyber Security and Types of Cyber Attacks', *International Journal of Advanced Research in Science, Communication and Technology*, pp. 732–735, Aug. 2022, doi: 10.48175/ijarsct-7043.

FINAL GRADE

GENERAL COMMENTS

Instructor

95/100

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project Excellent introduction. Suitable/ appropriate title. Aim and objectives well set.	20	19
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts Adequate literatures referred to the work. Could have added more critical reviews. Ethical Issues: Collecting anonymous data. What kind of d	20	18

ata are you planning to collect? How anonymous? Did you get a consent to gather data?		
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed The statement was clear and precise. Project design could have outlined the use of different OSs like windows server/ client/ Android/ Attacker etc.	30	28
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Resources and planning done appropriately.	15	15

Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit	15	15
Well Documented. In-text citation done.		
TOTAL	100	95

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9