WEBSITE DETECTION FOR PHISHING ATTACK BY USING BROWSER EXTENSION

PUTERA NURIQMAR ISKANDAR BIN AHMAD BASRI

Bachelor of Computer Science
(Computer System and Networking)

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesi is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Computer System and Networking)

(Supervisor's Signature)

Full Name : DR. JAMALUDIN BIN SALLIM

Position : SENIOR LECTURER

Date : 2 JANUARY 2019

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : PUTERA NURIQMAR ISKANDAR BIN AHMAD BASRI

ID Number : CA15060

Date : 2 JANUARY 2019

WEBSITE DETECTION FOR PHISHING ATTACK BY USING BROWSER EXTENSION

PUTERA NURIQMAR ISKANDAR BIN AHMAD BASRI

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science(Computer Science and Networking)

Faculty of Computer & Software Engineering

UNIVERSITI MALAYSIA PAHANG

DECEMBER 2018

ACKNOWLEDGEMENTS

All praise to Allah S.W.T for His blessing which has given me strength, patient, and ability to do my final year project along the period. I want to thank you my supervisor Dr. Jamaludin Bin Sallim for the guidance throughout this final year project 1. The idea and advice from Dr. Jamaludin Bin Sallim have made me done this research even though there is some challenge that I face when this research do. He gave insightful comments, outstanding advice, and exceptional guidance. I would also like to express my appreciation for his patience in spending a lot of time to guide me in my final year project and provide a lot of valuable and practical suggestion during the period. Not to forget my parents that always supportive to me by give motivation and my father supported me financial during this final year project. Lastly I want to thank my friends that always help when I down and guide me give some advice to motivate me to finish this final year project.

ABSTRAK

Internet adalah rangka kerja seluruh dunia yang boleh digunakan untuk perkongsian data, memberikan keseluruhan pentadbiran dan surat-menyurat. Walau bagaimanapun terdapat masalah dari segi keselamatan. Dalam tesis ini, kami memberi tumpuan kepada serangan pancingan data. Phishing adalah perangkap jenayah untuk mengambil data individu yang tidak disengajakan dengan menghantarnya e-mel yang spoofed mendorong mereka untuk melawat laman web yang dihasilkan yang menyerupai organisasi asli yang tulen dan meminta agar benefisiari memasukkan data individu, contohnya, nombor Mastercard, kata rahsia dan sebagainya. Masalah semasa yang berlaku adalah implan sambungan dalam e-mel yang dialihkan ke tapak yang tidak diingini yang menuntut data yang halus. Mengesampingkan penghantar menghantar e-mel untuk muncul sebagai sumber yang dihormati dan menuntut data yang halus. Objektif utama penyelidikan ini adalah untuk menyiasat serangan phishing adalah untuk menyiasat kaedah semasa serangan phishing, untuk mencadangkan susunan pendedahan susunan yang bergantung kepada peringatan pelanjutan penyemak imbas, untuk menilai serangan pemeriksaan susunan yang disyorkan bergantung pada penyemak imbas laman web. Metodologi yang digunakan dalam kajian ini adalah perancangan pertama, analisis fasa kedua, pelaksanaan fasa ketiga, kesimpulan fasa keempat dan fasa terakhir adalah dokumentasi. Hasil kajian ini menunjukkan bahawa pendekatan asas peraturan menguruskan untuk mengesan laman web pancingan data yang juga berkaitan dengan pangkalan data phishitank. Terdapat 3 peraturan yang telah digunakan dalam kajian ini daripada 14 peraturan. Selepas menjalankan pelanjutan, "Mod pemaju" mesti diaktifkan terlebih dahulu kerana pelanjutan yang dibuat ini adalah pelanjutan yang tidak dipunggah dan tambahan pula tidak mendaftar dalam Google Chrome. Dari peperiksaan ini, jelas bahawa rangka kerja yang dibina diaktualisasikan dengan menggunakan sambungan dalam Google Chrome. Kesimpulannya, matlamat tesis ini telah dicapai dengan menguji rangka kerja dalam pelayar internet Google Chrome.

ABSTRACT

Internet is a worldwide framework that can be utilized for sharing data, giving overall administrations and correspondence. However there are problem in term of security. In this thesis we focus on phishing attack. Phishing is a criminal trap of taking unfortunate casualties individual data by sending them spoofed email encouraging them to visit a produced site page that resembles a genuine one of an authentic organization and requests that the beneficiaries enter individual data, for example, Mastercard number, secret word and so forth. The current problem that occur are implanting a connection in an email that diverts to an unbound site that demands delicate data. Satirizing the sender deliver in an email to show up as a respectable source and demand delicate data. The main objective of this research is to investigate phishing attack are to investigate current method on phishing attack, to propose the arrangement exposure assault dependent against the browser extension alert, to evaluate the suggested arrangement inspection assault dependent on the website browser. The methodology that been use in this research is first planning, second phase analysis, third phase implementation, fourth phase conclusion and last phase is documentation. The result of this research show that rule base approach manage to detect the phishing website which are also connected to phishitank database. There are 3 rule that been use in this research out of 14 rule. After running the extension, "Developer mode" must be activated first since this made extension is an unloaded extension and furthermore not enlisted yet in Google Chrome. From this examination, it is clear that the built framework is actualized by utilizing extension in Google Chrome. In Conclusion, the goal of this thesis has been achieved by testing the framework in the Google Chrome internet browser.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

LIST OF ABBREVIATIONS

URL	Uniform Resource Locator
DNS	Domain Name System
IP	Internet Protocol
ARPANET	Advanced Research Projects Agency's Wide Area Network
SVM	Support Vector Machine
DOS	Denial of Services
SDLC	Software Development Life Cycle
DOM	Document Object Model
HTTP	HyperText Transfer Protocol
UMP	Universiti Malaysia Pahang

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet is a worldwide framework that can be utilized for sharing data, giving overall administrations and correspondence. Every day refreshes are effortlessly and quickly accessible in the web. Additionally, it can scan for any data that it are searching for; in the web. In this day and age, all organizations can work just with the utilization of web. A great deal of items and administrations are sold and gave through web today. Some time ago, phone was viewed as a quick method of correspondence. Presently, web has immensely developed and supplanted phone as quick method of correspondence.

However, even the internet give many benefit to humankind there is threat to people in terms of security. What the meaning of security is about the data of person whether it safe or not. The common security issue that famous and still relevant is phishing attack. Phishing is a criminal trap of taking unfortunate casualties individual data by sending them spoofed email encouraging them to visit a produced site page that resembles a genuine one of an authentic organization and requests that the beneficiaries enter individual data, for example, Mastercard number, secret word and so forth. The unfortunate casualties may at long last endure misfortunes of cash or different sorts. As per the reports of Anti-Phishing Working Group, the quantity of phishing assaults is expanding by month to month and they can more often than not persuade of the phishing email beneficiaries to react to them.

Furthermore, phishing is a criminal instrument utilizing both social designing and specialized subterfuge to take consumers‟ individual personality information and money related record qualifications, as per AntiPhishing Working Group (APWG). Phishing

messages for the most part follow up in the interest of a confided in outsider to trap email beneficiaries into playing out a few activities, for example, giving ceaselessly close to home data, e.g. financial balances, government managed savings numbers, usernames and passwords to internet saving money and well known long range interpersonal communication sites like Facebook, Twitter, and so on. In spite of the fact that much research on hostile to phishing procedures has been done and new systems and approaches are being proposed frequently, online con artists figure out how to think of creative plans to go around existing recognition innovations and draw potential unfortunate casualties to their phishing efforts.

In this paper, we propose ruled-based approach with recognizing phishing website pages and present our starter test results will investigate the phishing assault by means of Chrome Extension that will created for this research.

1.2 Problem Statement

The current problem for phishing attack.

I. Implanting a connection in an email that diverts to an unbound site that demands delicate data.

II. Satirizing the sender deliver in an email to show up as a respectable source and demand delicate data.

1.3 Objective

The main objective of this research is to investigate phishing attack:-

i. To investigate current method on phishing attack
ii. To propose the arrangement exposure assault dependent against the browser extension alert.
iii. To evaluate the suggested arrangement inspection assault dependent on the website browser.

1.4 Scope

The scope for this research are

i. The investigation using the extension to detect phishing website.

ii. The extension will focus on google chrome type of extension.

iii. The extension will use phishiTank as database.

1.5 Significance

i. The research is beneficial to society that give awareness about the important of security issue when come to phishing attack.
ii. To educate user about the benefit using browser for detection of phishing attack.

1.6 Thesis Organization

There will have five section in this thesis. Right off the bat, part one which is the introduction about what are the new innovation that can be enhance in our life. In this part it is additionally incorporates target of the exploration to accomplish the change of innovation. Others, there are likewise have issue articulation, extension and postulation association. All through this section, issue explanations will be distinguished where it prompts improvement to discover an answer for the research.

Next, section is about literature review directed to get some answers concerning research data. Writing survey incorporate the presentation of research examines when all is said in done, strategies or advancements that are fitting to meet the research.

At that point, section three talks about the methodology to be utilized as a part of research advancement and the general approach about what we will be utilized to create to this exploration. Through this part, a strategy will be chosen for the advancement of the framework that will be depicted and clarified. This part will likewise specify presentations, equipment, programming and Gantt outlines for use in the exploration in more detail.

REFERENCES

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based Associative Classification data mining. *Expert System with Application*.

Aldwairi, M., & Alsalman, R. (2012). MALURLS: A Lightweight Malicious Website Classification Based on URL Features. *JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE*, 128-133.

Alkhozae, M. G., & Batarfi, O. A. (2011). Phishing Website Detection based on Phishing Characteristic in the Webpage Source Code.

Alosefer, Y., & Rana, O. (n.d.). Honeyware: a web-based low interaction client honeypot.
Forcadi, R., & Tempesta, M. (n.d.). Development of security extensions based on Chrome APIs.

John, G. H., & Langley, P. (1995). Estimating Continuous Distributions in Bayesian Classifiers. *Proceedings of the Eleventh conference on Uncertainty in artificial intelligence* (pp. 338-345). Morgan Kaufmann Publishers Inc..

Kapravelos, A., Grier, C., Chachra Neha, & Kruegel, C. (2014). Hulk: Eliciting Malicious Behavior in Browser Extensions. *Proceedings of the 23rd USENIX Security Symposium* (p. 8). San Diego, CA: USENIX.

Koza, J. R., Keane, M. A., Streeter, M. J., Mydlowec, W., Yu, J., & Lanza, G. (2006). *Genetic programming IV: Routine human-competitive machine intelligence*. Springer Science & Business Media.

Pan, Y., & Ding, X. (2006). Anomaly Based Web Phishing Page Detection. *Proceedings of the 22nd Annual Computer Security Aplication Conference.* Computer Society

S. Doshi, N. Provos, M. Chew, and A. D. Rubin, "A Framework for Detection and Measurement of Phishing Attacks," in Proc. ACM Workshop on Rapid Malcode (WORM), Alexandria, VA, Nov. 2007

R. B. Basnet, S. Mukkamala, and A. H. Sung, Detection of phishing attacks: A machine learning approach. Studies in Fuzziness and Soft Computing, 226:373-383, Springer, 2008.

PhishTank – Statistics about phishing activity and PhishTank usage. [Online]. Available: http://www.phishtank.com/stats.phphttps://www.wandera.com

Ram B. Basnet, Andrew H. Sung, Quingzhong Liu, Ruled-Based Phishing Attack Detection, *Department of Computer Science, Sam Houston State University, Huntsville*, TX 77341, USA, 2012.