Pen-Testing Investigation Report

Name: Ray Parker

Student ID: 10532682

Unit Coordinator:

CYB6006 Ethical Hacking and Defence

Semester X -2021

School of Science – Computing and Security

Edith Cowan University, Joodalup Campus

Table of **Contents**

[Executive Summary 2](#_Toc99127488)

[Objective 2](#_Toc99127489)

[Scope 3](#_Toc99127490)

[Methodology 3](#_Toc99127491)

[Testing /Revision Log 4](#_Toc99127492)

[Next Steps 4](#_Toc99127493)

[References 4](#_Toc99127494)

## Executive Summary

**The contents of this document and private and confidential. If you do not have authorization from the owner of this document you are prohibited from reading it.**

**Text-based passwords alone are subject to dictionary attacks as users tend to choose weak passwords in favor of memorability, as well as phishing attacks. Many recognition-based graphical password schemes alone, in order to offer sufficient security, require a number of rounds of verification, introducing usability issues. We suggest a hybrid user authentication approach combining text passwords, recognition-based graphical passwords, and a two-step process, to provide increased security with fewer rounds than such graphical passwords alone. A variation of this two-step authentication method, which we have implemented and deployed, is in use in the real world (Method & Passwords, 2009).**Objective

The results of this prototype test is to facilitate a positive login result from the 2 step authentication process that will be utilised network wide across the entire company

need to refine this executive summary

**Text passwords have been widely used for user authentication, e.g., by almost all websites on the Internet. However, it is well-known that text passwords are insecure for a variety of reasons. For example, users tend to choose simple passwords in favour of memorability, making them subject to dictionary attacks; and text passwords can be stolen by malicious software (e.g., keystroke loggers) when being entered from keyboards. Phishing is another serious threat to text passwords, by which, a user could be persuaded to visit a forged website and enter their passwords. Such an attack is made possible in part due to the fact that text passwords do not allow users to authenticate a server; by design they provide only one-way user authentication, and server authentication is not a design objective of text passwords alone. We propose a two-step authentication method to strengthen text passwords by combining them with graphical passwords. In this approach, called TwoStep, users continue to use text passwords as a first step, but then must also enter a graphical password, providing the following advantages: (1) users’ current sign-in experience is largely preserved; (2) a text password alone which is stolen (e.g., by phishing) does not compromise an account; (3) users can be alerted if not seeing the graphical password cuing image after providing their text passwords, implicitly providing server authentication; and (4) it can be implemented in software alone, increasing the potential for large-scale adoption on the Internet**

## Scope

2SAS Two Step Authentication Solution: Passwords with access to organizational systems and networks are vulnerable and open to hackers and compromise the network system. Many organizations fail to secure or implement strong passwords for users. To harden the computer network in the organization we plan to introduce a simple one button press token to generate a pin number to use with the user password to gain access to the system. The use of a sms solution requires all users to have their phone with them at login. This presents a problem when you consider many government and military organisations prohibit the use of mobile phones in the office or in some cases the building.

Manage the password authentication process to harden the computer system to protect from attacks and hackers gaining access to the network system.

## Methodology

The following features are proposed:

* The stakeholders require a more secure login system to prevent attacks from internal and external actors.
* Users will provide a password along with a pin generated by the dongle to login to the network system.
* This solution will harden the network system and help protect assets and intellectual property from attacks.
* Users will not be impacted except for an extra 5 seconds to input the pin to login.
* The only cost incurred by the stakeholders will be the purchase of the dongle
* This solution will only require existing IT personnel to implement the change necessary on the server side to include the scripting to allow authentication for user logins.

## This project will be implemented over a period of 18 weeks from January 10 2022 and is expected to be completed by 26 June 2022 (Parker, 2022).

The resources required to complete this project include the purchasing of the dongle to be used and supplied to all users of the system. An inventory system will be integrated into the current asset inventory system to allocate the dongles to users of the network.

Current IT department employees will be provided by the company eliminating any new costs to the project.

A video presentation will be created in order to show the stakeholders how the new system will operate and the new login process will only add around 5 seconds to the current login time.

Training users will only include a short explanation of how to use the new dongle to generate the pin which expires in 5 seconds and a new pin is generated to operate in sync with the authentication server.

## 

## Testing/Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | **Action** | **Steps performed** | **Results (If any)** |
| 2 | Opened Kali Linux VM | Opened Kali Linux VM in VMWare | Kali Linux VM initialised |
| 3 | Opened Case Study VM | Opened Kali Linux VM in VMWare | IP address: 192.168.46.131   Subnet mark: 255.255.255.0  Noted CIDR from subnet mask of /24 |
| 4 | Opened Case Study VM | Entered terminal command (Kali Linux):  **ifconfig** | IP addresses found: 192.168.46.1 192.168.46.2  192.168.46.130 192.168.46.131 192.168.46.254 |

## Next Steps we need to define this part of the doc

## References

Method, T. A. A., & Passwords, C. T. a. G. (2009). TwoStep An Authentication Method.

Parker, R. (2022). *CYB6013\_Prototype Activity Report*.