ASSESSMENT 3: PROTOTYPE ACTIVITY REPORT

CYB6013 CYBER PROJECT 2

Name: Ray Parker

Student ID: 10532682

Unit Coordinator: BAZLUR RASHID

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 5](#_Toc99127492)

[Next Steps 6](#_Toc99127493)

[References 6](#_Toc99127494)

## Executive Summary

Creating this virtual network to conduct extensive testing of the 2 step authentication process will allow transcend IT Services to run unlimited tests in a live virtual environment without any impact on the current network system and will not interrupt day to day operations of the company and will provide real time visual feedback to the client and show the new login solution operational (Parker, 2022).

## **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

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 (Method & Passwords, 2009). We propose a two-step authentication method to strengthen text passwords by combining them with pin generated dongle. In this approach, called Twostep Authentication, users continue to use text passwords as a first step, but then must also enter a pin number generated from a dongle, 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 cueing 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 (Method & Passwords, 2009).

## 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.

Accessibility features will be a prominent addition to this project given the amount of potential users in the workforce with disabilities. Every user of this system will now be a stakeholder. Windows sever and workstation software already includes the Narrator, Magnifier and Screen Enlargers. Screen magnifiers work like a magnifying glass by enlarging a portion of the screen as the user moves the focus. Voice input aids or speech recognition assist people who have difficulty using a mouse or keyboard. Voice aids allow users to control computers with their voice instead of a mouse or keyboard. Screen reviewers and screen readers make on-screen information available as synthesized speech or a refreshable Braille display. An on-screen keyboard can help those unable to use a standard keyboard select keys using a pointing method such as pointing devices, switches, or Morse-code input systems. Keyboard enhancement utilities help those with trouble typing--including increasing typing speed. Assistive technology can compensate for erratic motion, tremors, slow response time, and other related conditions (Camen Lamboy, 2002).

Users with impairments will have access to all the accessibility features built into the windows operating system which are available at the login screen. Manage the password authentication process to harden the computer system to protect from attacks and hackers gaining access to the network system.

## Methodology

To prepare a virtual lab consisting of 2 servers running Microsoft Server 2022 and 5 client machines running Microsoft Windows 11 mentioned in the preceding table 1. Evaluation ISO images (Windows Server 2022 (Insider Preview) and Windows 11\_English) from the Microsoft Evaluation download centre. VM Ware Workstation software was provided by ECU university, downloaded and installed on the host machine (Dell 9010 SSF workstation). The first virtual machine which will be the first Domain Controller (DC01) was created in VMWare. Installation was performed by an automated .xml file. Once installed this server was promoted as a Domain Controller in the widget LLC forest with Active Directory services installed. The second Domain Controller (DC02) was then installed in Vmware and promoted to the widget LLC domain (K.G.Mark, 2016).

Two-factor authentication is a part of modern authentication technologies. It is also called multifactor authentication or in short 2FA. Traditional one-factor authentication process provides only one factor, typically something on what an individual can memorize. Personal numbers (PIN) and passwords are typical examples of this kind of authentication methods. Two-factor authentication needs more challenge from the individual. This authentication is based in the assumption that two of the three factors of authentication are used. For this project we will use the authentication process of a password and pin number generated by a dongle to authenticate the user credentials (Kymäläinen, 2018).

|  |  |  |
| --- | --- | --- |
| **Step.No.** | **VM Name** | **Operating System** |
| 1 | DC01 | Windows Server 2022 |
| 2 | DC02 | Windows Server 2022 |
| 3 | Client01 | Windows 11 Pro |
| 4 | Client02 | Windows 11 Pro |
| 5 | Client03 | Windows 11 Pro |
| 6 | Client04 | Windows 11 Pro |
| 7 | Client05 | Windows 11 Pro |

*Table 1.*

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **VM Name** | **IP Address** | **Role** |
|  | DC01 | 10.10.10.101  Netmask :255.0.0.255  DNS: 10.10.10.100 | Domain Controller of widgetllc.internal domain. |
| 2 | DC02 | 10.10.10.102  Netmask :255.0.0.255  DNS: 10.10.10.100 | Member sever of widgetllc.internal domain. |
| 3 | Client01 | 10.10.10.103  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 4 | Client02 | 10.10.10.104  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 5 | Client03 | 10.10.10.105  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 6 | Client04 | 10.10.10.106  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 7 | Client05 | 10.10.10.107  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |

*Table 2.*

Restart and sign in to the system with the Administrator account. After some time, the Server Manager console will display. 4. Open the Run dialog box, type ncpa.cpl, and then press Enter. 5. Select and right-click the active network adapter, and then select Properties. 6. Set the following TCP/IP settings: IP address: 10.0.0.100. Subnet mask: 255.0.0.0. Default gateway: 10.0.0.1. Preferred DNS server: 10.0.0.100The 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

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Action** | **Steps performed** | **Results (If any)** |
| 1 | Install Windows Server 2022 in VM Ware as Domain Controller 1(DC01) | Opened VM ware on Host Dell 9010 | VM workstation initialised |
| 2 | Promote Server DC01 with Active Directory Services | Promote DC01 primary DC in widgetllc forest | IP address: 10.10.10.101 Subnet mask: 255.0.0.0  DNS: 10.10.10.100 |
| 3 | Install Windows Server 2022 in VM Ware as Domain Controller 2 (DC02) | Promote DC02 into the widgetllc forest | IP address: 10.10.10.102 Subnet mask: 255.0.0.0   DNS: 10.10.10.100 |
| 4. 09/04/2022 | At the login screen  Press ctrl alt delete to bring up the login screen | Enter your password and generated pin | Login successful |
| 5 | At the login screen  Press ctrl alt delete to bring up the login screen | Login successful | Login successful |
| 6 10/04/2022 | At the login screen  Press ctrl alt delete to bring up the login screen | Login successful | Login successful |
| 7 | At the login screen  Press ctrl alt delete to bring up the login screen | Login successful | Login successful |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |
| 16 |  |  |  |
| 17 |  |  |  |
| 18 |  |  |  |

## Next Steps

## we need to define this part of the doc

## 

## References

Camen Lamboy, M. S. (2002). Microsoft Windows XP Accessibility Features.

K.G.Mark. (2016). Installing and Configuring Windows Server 2016 (Hands-on Guide).

Kymäläinen, J. (2018). Implementing Two-Factor Authentication.

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

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