ASSESSMENT 3: REPORT AND ACTION PLAN

CYB6014.2 CYBER PROJECT 3

Name: Ray Parker

Student ID: 10532682

Unit Coordinator: BAZLUR RASHID

School of Science – Computing and Security

Edith Cowan University, Joondalup Campus

Table of **Contents**

[Executive Summary 3](#_Toc99127488)

[Objective 3](#_Toc99127489)

[Scope 4](#_Toc99127490)

[Methodology 5](#_Toc99127491)

[Testing /Revision Log 6](#_Toc99127492)

[Next Steps 10](#_Toc99127493)

[References 10](#_Toc99127494)

## Executive Summary

The 2 step authentication login process proposed in this document is designed to make company login information more secure from outside or external attacks from unscrupulous actors or scammers trying to penetrate corporate networks for financial or malicious purposes. This 2 step process requires the user to input a password and pin number generated from a dongle to access the corporate network. Several companies, Government and Military groups do not allow mobile telephones or other electronic devices inside the building or workplace thus eliminating the transmission of an sms pin number being sent to the user to complete this type of authentication. For this project we created a virtual lab mimicking a live network environment to test and retest the login process to make sure the process was as secure a possible before migrating over to the live system. Normal network issues were encountered during this process and should not have any impact once introduced into the live environment. The overall process only adds about 5 seconds to the login process and will not have any significant impact on current users. Accessibility features included in the windows operating system login screen will help users with impairments alleviate most of the difficulties associated with eyesight and hearing issues.

## **Objective**

The objective of this prototype is to provide a more secure solution to the login process. A password and pin generated from a dongle will be utilised for the login process. The results of this prototype tests are to facilitate a positive login result from the 2 step authentication process that will be utilised network wide across the entire company.

## 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.

## 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 following table 1. Evaluation ISO images (Windows Server 2022 (Insider Preview) and Windows 11\_English) were downloaded 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 (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 processes provide only one factor, typically something on what an individual can memorize. Personal numbers (PIN) and passwords are typical examples of these kinds of authentication methods. Two-factor authentication needs more input from the individual. This authentication is based on 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 | 192.168.1.222  Netmask :255.255.255.0  DNS: 192.168.1.1 | Domain Controller of widgetllc.internal domain. |
| 2 | DC02 | 192.168.1.223  Netmask :255.255.255.0  DNS: 192.168.1.1 | Member sever of widgetllc.internal domain. |
| 3 | Client01 | 192.168.1.225  Netmask :255.255.255.0  DNS: 192.168.1.1 | Client machine of widgetllc domain |
| 4 | Client02 | 192.168.1.226  Netmask :255.255.255.0  DNS: 192.168.1.1 | Client machine of widgetllc domain |
| 5 | Client03 | 192.168.1.227  Netmask :255.255.255.0  DNS: 192.168.1.1 | Client machine of widgetllc domain |
| 6 | Client04 | 192.168.1.228  Netmask :255.255.255.0  DNS: 192.168.1.1 | Client machine of widgetllc domain |
| 7 | Client05 | 192.168.1.229  Netmask :255.255.255.0  DNS: 192.168.1.1 | Client machine of widgetllc domain |

*Table 2.*

## Testing/Revision Log

## The virtual environment setup utilised server domain controllers with the password of (PASSWORD123!) for both domain controller included in the autounattend .xml script. The five workstation were built utilising the password of (J388ica\*) across all five workstations.

## Next Steps

## I found this process very time consuming given the nature of software complexities and small errors encountered. Next steps include finding a way to automate this process. Although we had time constraints with this project I believe some extra time spent with planning would benefit similar projects in the future. Future solutions to harden networks include a Voice or IRIS Scan option keeping this process a 2 step process or making it a 3 step login process.

**Goal of the Project**

The goal of this project is to deliver a more secure login solution the client to prevent unauthorised access to the corporate network system. At this stage the prototype is progressing very well with only minor problems in relation to the acquisition of a dongle to proceed with testing.

**Deadlines and Milestones**

Milestones so far have been reached and only final product testing is incomplete. At his point in time we are on schedule and will meet our deadline on time

**Statement of work Required**

This project includes a 2 step logon authentication using a password and pin generated from a dongle to access the corporate network. The purpose of the project is to harden the security of the corporate network to protect against theft and attacks internal and external actors.

## References

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

Kymäläinen, J. (2018). Implementing Two-Factor Authentication. <https://www.theseus.fi/bitstream/handle/10024/145670/Thesis_Jori_Kymalainen.pdf?sequence=1&isAllowed=y>

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