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, Joondalup Campus

Table of **Contents**

[Executive Summary 2](#_Toc99127488)

[Objective 2](#_Toc99127489)

[Scope 3](#_Toc99127490)

[Methodology 3](#_Toc99127491)

[Testing /Revision Log 6](#_Toc99127492)

[Next Steps 11](#_Toc99127493)

[References 12](#_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 are 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 Two-step 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 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.

## 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, DHCP and DNS 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 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 | 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.*

Open the Virtual Lab Environment and start the servers and login to initiate the lab environment. Start one of the client machines – Client01.

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

## 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.

|  |
| --- |
| ***Task 1: Installing VMware Workstation on the Host Machine*** |
| To Install VMware Workstation or VMware Player, first you need to download it.  Once it is downloaded, just double-click the setup file, and follow the simple steps to complete the installation process |
| ***Task 2: Installing and Configuring the DC01 Virtual Machine*** |
| To install and configure the Domain Controller (DC01) virtual machine, you need to perform the following steps: |
| 1. Make sure that the VMware console is active. |
| 2. Select File and then select New Virtual Machine. |
| 3. On the New Virtual Machine Wizard, click Next. |
| 4. On the Guest Operating System Installation page, select the Installer disc image file (iso): radio button, browse the location of the Server 2022 ISO image file, and then click Next. |
| 5. Note: If you use the VMware platform that automatically detects the version of the Windows server, you may be asked to set the following settings: Product key Operating system edition Administrator password Otherwise, you may skip it. |
| 6. On the Select a Guest Operating System page, select the highest supported version of Windows server (in this case Windows Server 2022 or above but it will still support Windows Server 2022), and then click Next. |
| 7. On the Name and Virtual Machine page, type DC01 in the Virtual machine name field. |
| 8. In the Location field, navigate the location where you want to save the virtual machine, such as C:\Virtual Machines, and then click Next. |
| 9. On the Specify Disk Capacity page, select Store virtual disk as a single file, optionally you can also set the disk size as well, and then click Next. |
| 10. On the Ready to Create Virtual Machine page, click Customize Hardware. |
| 11. On the Hardware window, select Network Adapter in the left pane. Select the Host only radio button, and then click Close. |
| 12. Click Finish. |
| 13. On the VMware console, power on the DC01 virtual machine. |
| 14. On the Windows Setup page, click Next, and then click Install Now. |
| 15. On the Select the operating system you want to install page, select the Windows Server 2022 Desktop Experience, and then click Next. |
| 16. On the License terms page, select the “I accept the license terms” check box, and then click Next. |
| 17. On the Which type of installation do you want page, select the Custom option, and then click Next. |
| 18. On the Where do you want to install Windows page, click Next. |
| 19. The Installation process will begin, after 10-15 minutes the Customize settings screen will display. |
| 20. Set Administrator password as PASSWORD123! |
|  |
| ***Task 2.1: Configuring the DC01 Virtual Machine*** |
| 1. Sign in to DC1 with the Administrator account. |
| 2. Open the System Properties (sysdm.cpl) and set the computer name as DC01. |
| 3. Restart and sign in to the system with the Administrator account. After some time, the Server Manager console will display. |
| 3. 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: 192.168.1.222. Subnet mask: 255.255.255.0 Default Gateway: 127.0.0.1. Preferred DNS server: 192.168.1.1. |
| 7. Close the Network Connections console (Mark, 2016). |
|  |
| Task 1: Configuring DC01 as a Domain Controller without Installing the DNS Server Role |
| 1. Sign in to DC01 with the Administrator account. |
| 2. On the Server Manager console, click the Add roles and features link. |
| 3. On the Before you begin page of the Add Roles and Features Wizard, click Next. |
| 4. On the Select installation type page, click Next. |
| 5. On the Select destination server page, make sure that DC01.widgetllc.internal is selected, and then click Next. |
| 6. On the Select server roles page, select the Active Directory Domain Services check box. |
| 7. On the Add Roles and Features Wizard dialog box, click Add Features, and then click Next. |
| 8. On the Select features page, click Next. |
| 9. On the Active Directory Domain Services page, click Next. |
| 10. On the Confirm installation selections page, click Install. |
| 11. The installation process will start. Click Close, once the installation succeeded. |
| 12. On the Server Manager console, click the Notifications icon, and then click the Promote this server to a domain controller link, as shown in the following figure. |
| 13. On the Deployment Configuration page of the Active Directory Domain Services Configuration Wizard, make sure that the Add a new forest radio button is selected. |
| 14. Under the Supply the credentials to perform this operation section, click Change. |
| 15. On the Windows Security dialog box, in the User name text box, type MCSALAB\Administrator. In the Password text box, type Password123!. |
| 16. The Deployment Configuration page is returned, as shown in the following figure. Review the selected options, and then click Next. |
| 17. On the Domain Controller Options page, clear the Domain Name System (DNS) server check box. |
| 18. Under the DSRM password section, type Password123! in the Password and Confirm password text boxes, and then click Next. |
| 19. Click Next, until the Prerequisites Check page is displayed. |
| 20. On the Prerequisites Check page, click Install. |
| 21. The installation process will start and the server will restart automatically. |
| After DC01 restarts, sign in to DC01 with the WIDGETLLC\Administrator account. |
| **Task 2.2:** Promoting the DC01 Virtual Machine as a Domain Controller: To promote the DC01 virtual machine as a domain controller, you need to perform the following steps: |
| 1. Open the Server Manager console. |
| 2. Click the Add roles and features link. |
| 3. On the Before you begin page, click Next. |
| 4. On the Select installation type page, click Next. |
| 5. On the Select destination server page, click Next. |
| 6. On the Select server roles page, select the Active Directory Domain Services check box, as shown in the following figure. |
| 7. Accept the default selections through rest of the wizard and complete the installation process. |
| 8. Click Close, once the installation succeeds on DC01. |
| 9. On the Server Manager console, click the Notifications icon. |
| 10. Click the Promote this server to a domain controller link, as shown in the following figure. |
| 11. On the Deployment Configuration page, select the Add a domain controller to an existing forest radio button is selected. |
| 12. In the Root domain name text box, type widgetllc.internal, as shown in the following figure, and then click Next. |
| 13. On the Domain Controller Options page, make sure that the Domain Name System (DNS) server check box is selected, as shown in the following figure. |
| ***14.*** In the Password and Confirm password text boxes, type the Password123!, and then click Next. |
| ***15.*** On the DNS Options page and then click Next. |
| ***16.*** On the Additional Options page, click Next. |
| ***17.*** On the Paths page, as shown in the following figure, review the default location for the AD DS database file, and then click Next. |
| ***18.*** On the Review Options page, click Next. |
| ***19.*** On the Prerequisites Check page, as shown in the following figure, review the prerequisites, and then click Install. |
| **20.** After some time, the system will restart automatically; sign in to DC01 with the WIDGETLLC\Administrator account. |
| **21.** Do not shut down the DC01 virtual machine (Mark, 2016). |
| Task 3: Installing and Configuring the SERVER1 Virtual Machine To install and configure the DC01 virtual machine, you can follow the simple steps as you used to install and configure the DC01 virtual machine. |
| **1.** During the installing DC01 virtual machine, make sure that you use the following settings and options: Virtual machine name: DC01. Operating system version: Windows Server 2022. Memory: 2048 MB Hard disk size: 50 GB Network Adapter: Host only (click Customize Hardware before clicking the Finish button.) Password: PASSWORD123!. |
| ***2.*** Once you installed the DC01 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 192.168.1.222 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 Preferred DNS server: 127.0.0.1 |
| 3. Once you configured the preceding TCP/IP settings, open the System Properties dialog box and click Change. |
| 4. On the Computer Name/Domain Changes dialog box, in the Computer name text box, type DC01. |
| 5. Select the Domain radio button, in the Member of section, and then type widgetllc.internal, and then click OK. |
| 6. On the Windows Security dialog box, provide the credentials of the DC01 server, and restart the DC01 virtual machine. |
| 7. Sign in to DC01 with the Administrator account. |
| 8. Shut down the DC01 (Mark, 2016). |
|  |
| **Task 4: Installing and Configuring the CLIENT01 Virtual Machine** |
| To install and configure the CLIENT01 virtual machine, you can follow the simple steps as you used to install and configure the DC01 virtual machine. |
| 1. During the installing CLIENT01 virtual machine, make sure that you use the following settings and options: Virtual machine name: CLIENT01. Operating system version: Windows 10 or later 64bit. Memory: 1024 MB Hard disk size: 50 GB Network Adapter: NAT (click Customize Hardware before clicking the Finish button.) Password: J388ica\* |
| ***2.*** Once you installed the CLIENT01 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 192.168.1.230 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 Preferred DNS server: 127.0.0.1 |
| ***3.*** Once you configured the preceding TCP/IP settings, open the System Properties dialog box, and click Change. |
| 4. On the Computer Name/Domain Changes dialog box, in the Computer name text box, type CLIENT01. |
| ***5.*** Select the Domain radio button in the Member of section, type widgetllc.internal, and then click OK. |
| ***6.*** On the Windows Security dialog box, provide the credentials of the DC01 server, and restart the CLIENT01 virtual machine. |
| 7. Sign in to CLIENT01 with the Administrator account password: J388ica\*. |
| ***8.*** Shut down the CLIENT01 virtual machine. |
| Note:the above procedure can be used to install any other Client machines in the lab environment with changes made to each IP Address. |
| ***Task 6: Creating and Configuring the DC02 Virtual Machine*** |
| To install and configure the SERVER2 virtual machine, you can follow the simple steps as you used to install and configure the DC1 virtual machine. |
| ***1.*** During the installing SERVER2 virtual machine, make sure that you use the following settings and options: Virtual machine name: SERVER2. Operating system version: Windows Server 2016. Memory: 1024 MB Hard disk size: 50 GB Network Adapter: VMnet2 Password: PASSWORD123! |
| *2.* Once you installed the SERVER2 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 192.168.1.223 Subnet mask: 255.255.255.0 Default gateway: not set: Preferred DNS server: 192.168.1.1 |
| *3.* Once you configured the preceding TCP/IP settings, open the System Properties dialog box, set the computer name as DC02, and restart the DC02 virtual machine. |
| *4.* Sign in to DC02 with the Administrator account. |
| *5*. Shut down the DC02 virtual machine. |
|  |

## 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.

Mark, H. G. (2016). Installing and Configuring Windows Server 2016 Hands-on Guide\_ Step By Step Lab Guide.

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

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