Prototype_ Activity_Report_V1.4.docx

by Donald PARKER

Submission date: 11-Apr-2022 12:30PM (UTC+0800)
Submission ID: 1807448053
File name: Prototype__Activity_Report_V1.4.docx (42.05K)
Word count: 2737
Character count: 14598

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

2

Table of Contents

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.

Task 1: Installing VMware Workstation on the Host Machine
To Install VMware Workstation or VMware Player, first you need to download the software. Once it is downloaded, 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 this section.
6. On the Select a Guest Operating System page, select the highest supported version of Windows server (in this case Windows Server 2016 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 to the location where you want to save the virtual machine, such as C:\Virtual Machines, or select the default location 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 Activate Windows page type your serial number and click Next, 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!
21. Install VM Ware Tools in this Virtual Machine
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 3: Configuring DC01 as a Domain Controller.
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 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. in the Root Domain name section type widgetllc.internal or the name of your domain, click Next On the Domain Controller Options page type a DSRM password J388ica* and click Next
15. On the DNS page click Next, and on the Additional Options, click Next, On the Paths Page click

Next, Review Options, click Next, then click Install
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 4: Promoting the DC02 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 DC02.
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.
Task 5: 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: 192.168.1.225 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 Preferred DNS server: not set
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: Installing a login script to the DC01 domain Controller
A generic login script from Microsoft will be utilised in this Lab testing environment.
The login script is found in the C:\Windows\SYSVOL\widgetllc.internal\scripts folder and replicated to the C:\Windows\SYSVOL\Domain\scripts folder
Testing continued over several days with more positive results than negative with the procedure being one of the easiest processes so far in this project.
Task 7. Invite several users to test the new login process
5 users were randomly selected to participate in testing procedures and invited to go through the process.
1. A ten minute explanation and user documentation was given to all 5 users.
2. 1 user required further explanation for the vision impaired login process
3. All 5 selected users progressed through the testing phase without any issues

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.

References

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

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

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

Prototype_ Activity_Report_V1.4.docx

ORIGINALITY REPORT

61%	56%	20%	26%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	baixardoc.com Internet Source	45%
2	Submitted to Edith Cowan University Student Paper	5%
3	files.eric.ed.gov Internet Source	5%
4	alfafarhans.blogspot.com Internet Source	2%
5	Submitted to Victoria University Student Paper	1%
6	www.theseus.fi Internet Source	1%
7	protechgurus.com Internet Source	1%
8	m.everything2.com Internet Source	1%
9	www.marcoprotasi.it Internet Source	<1%

10	www.pdf-archive.com Internet Source	<1%
11	docshare.tips Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		