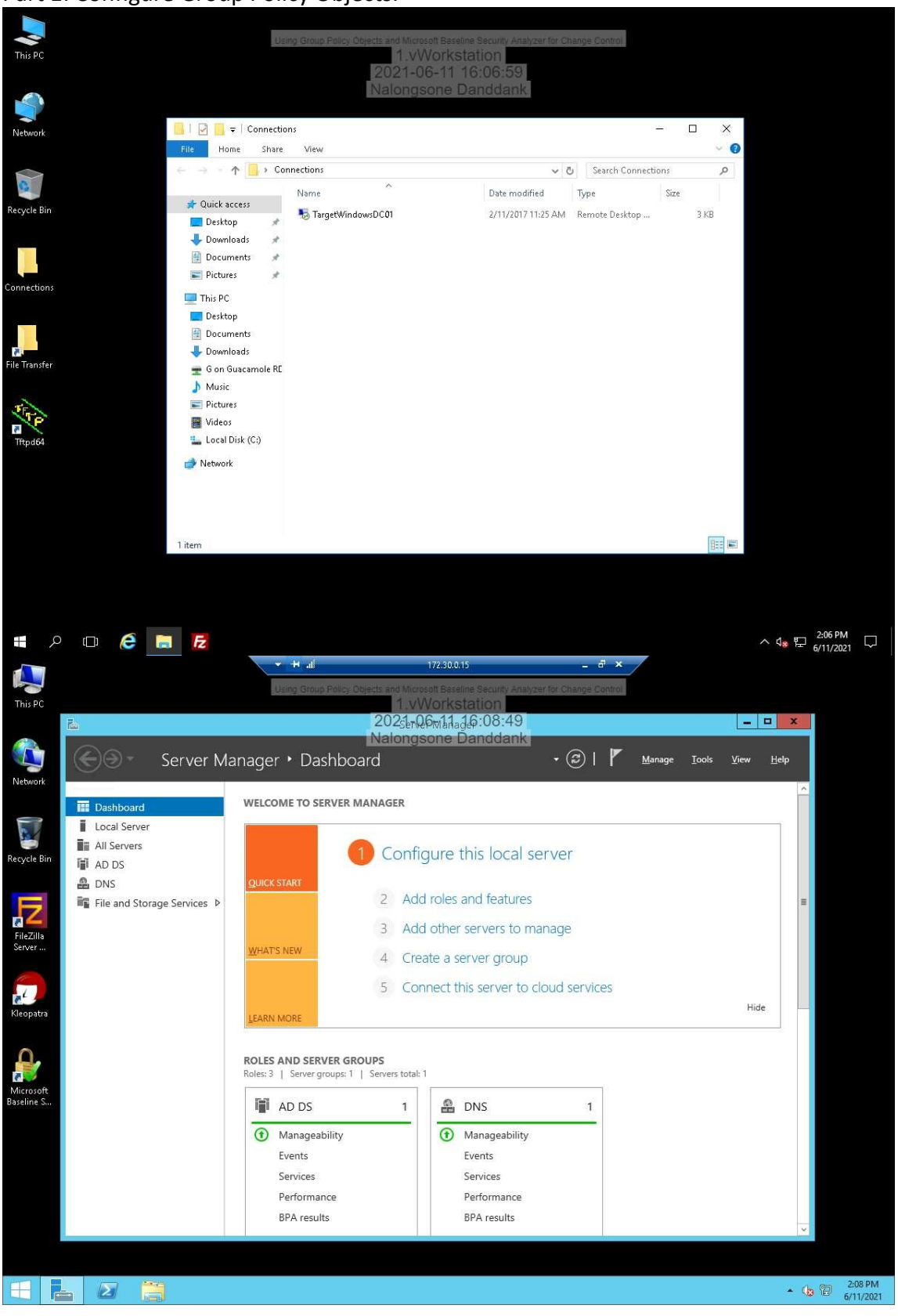
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

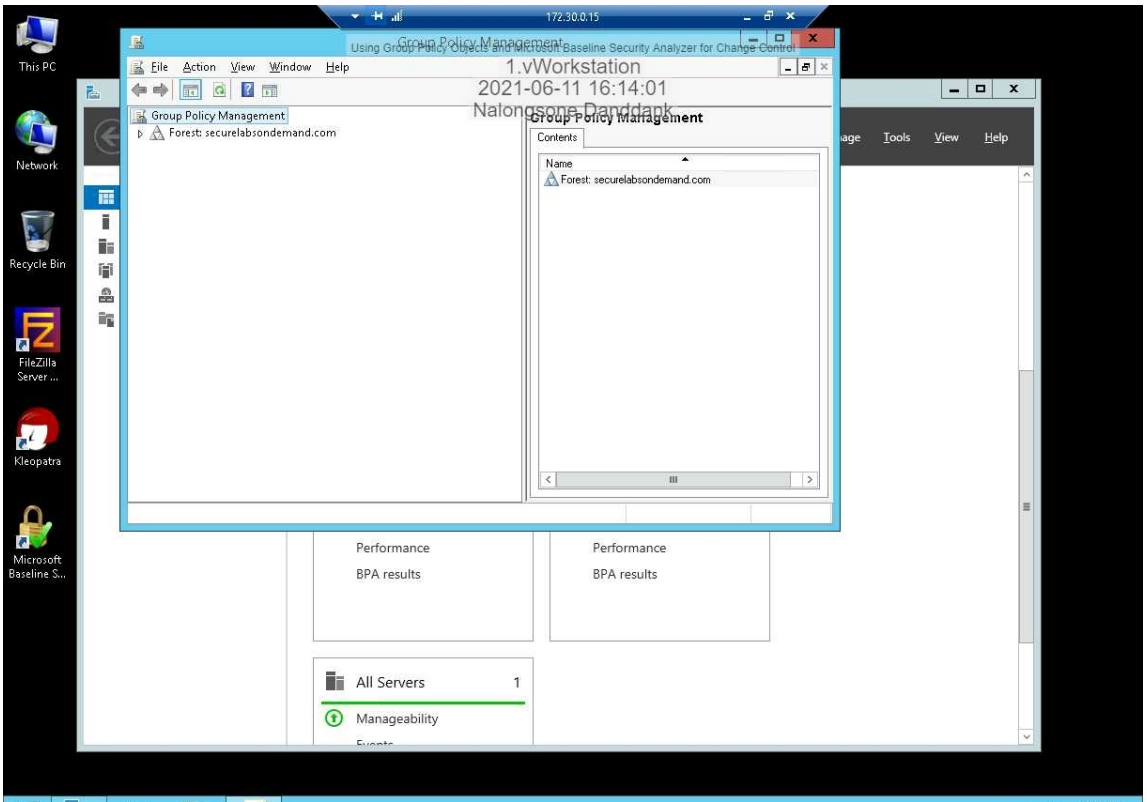
**ICS382/CYBR332-51 —Computer Security**

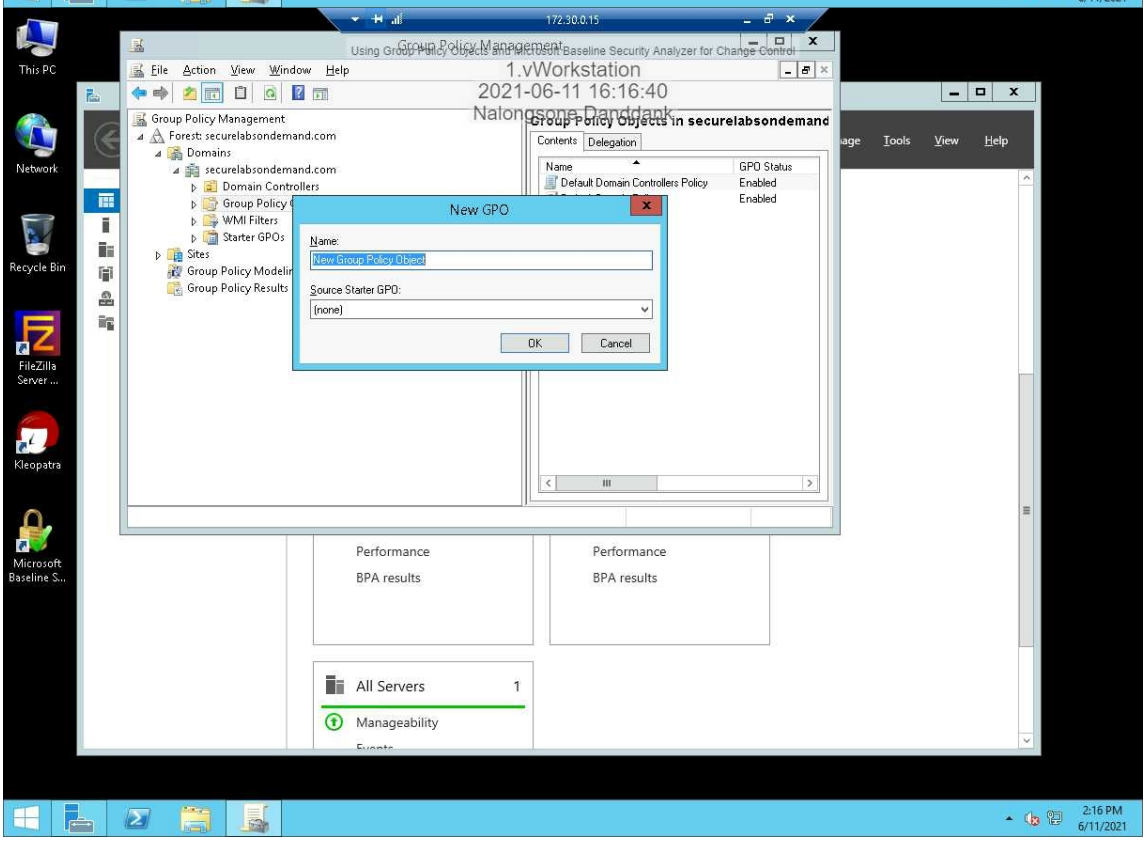
**Lab #4 Report**

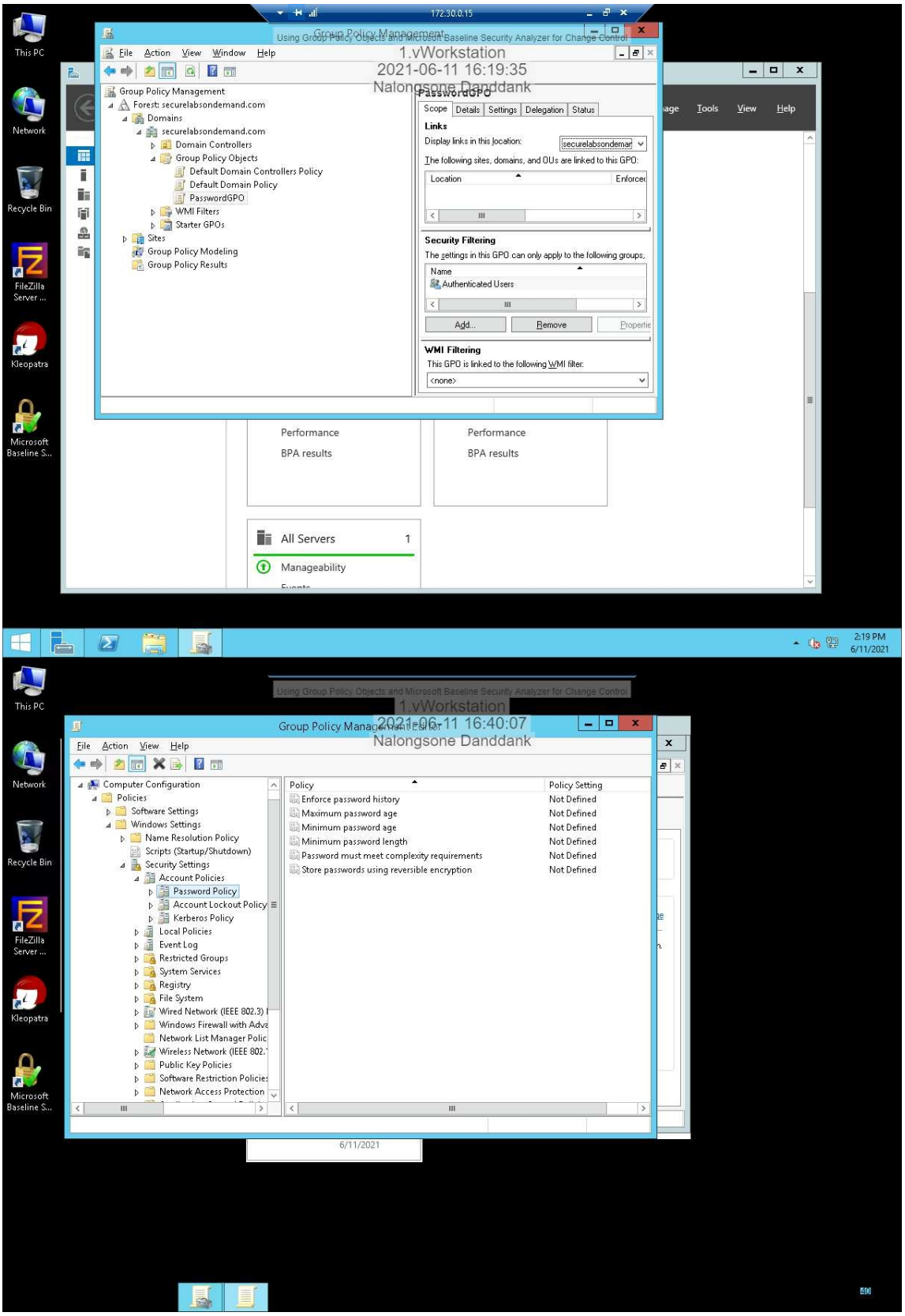
# Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control

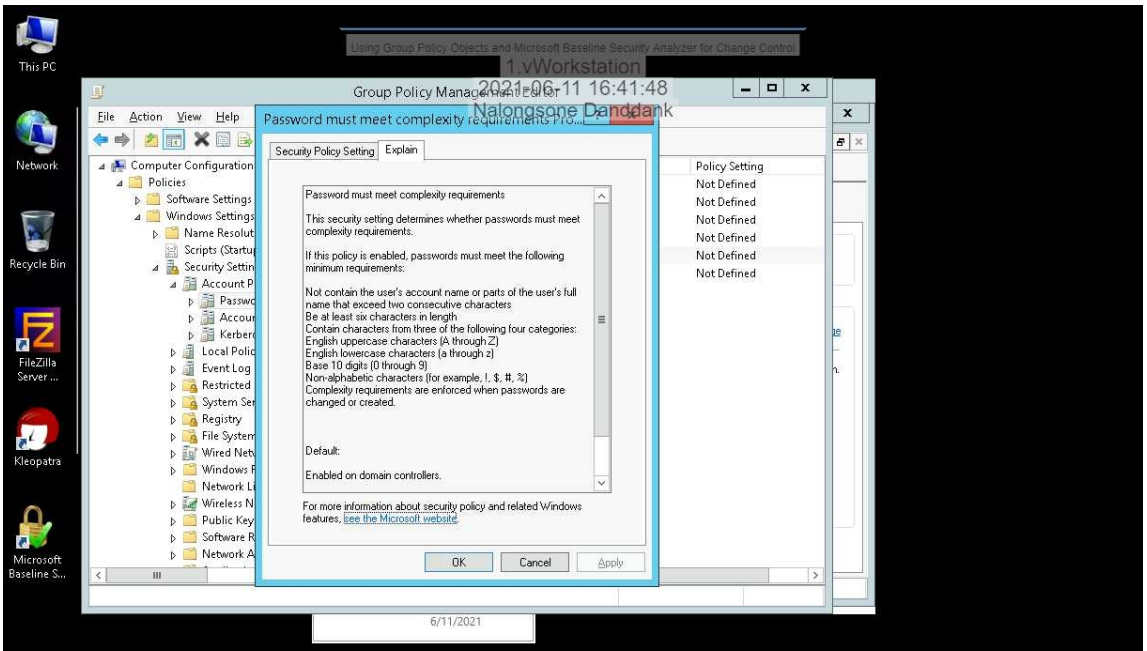
Part 1: Configure Group Policy Objects.

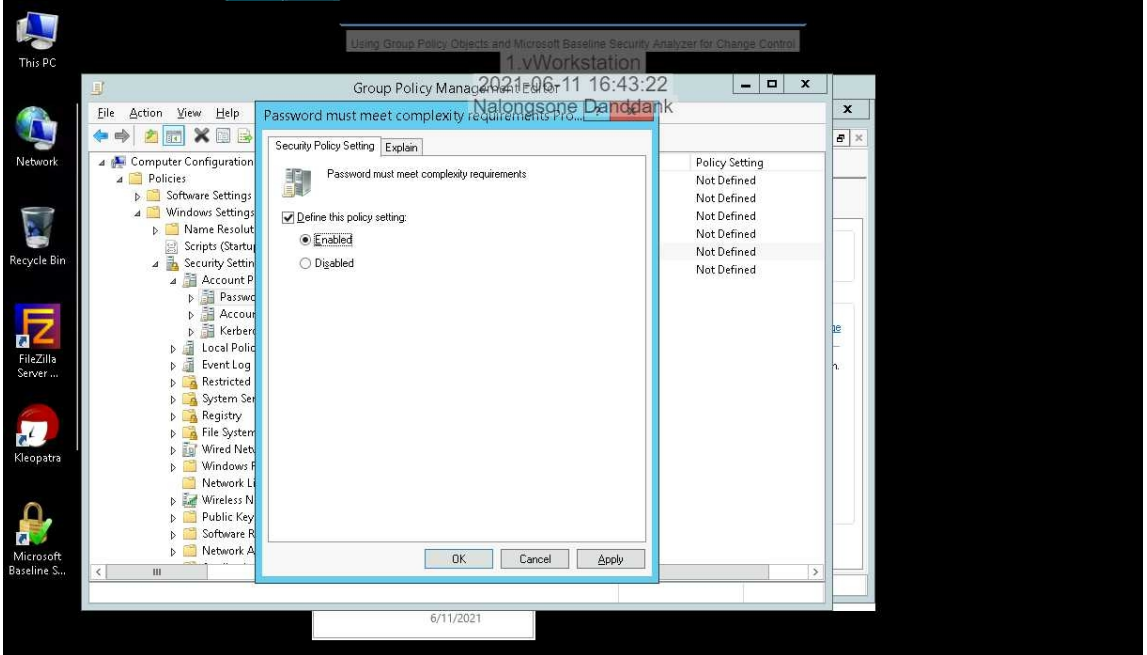


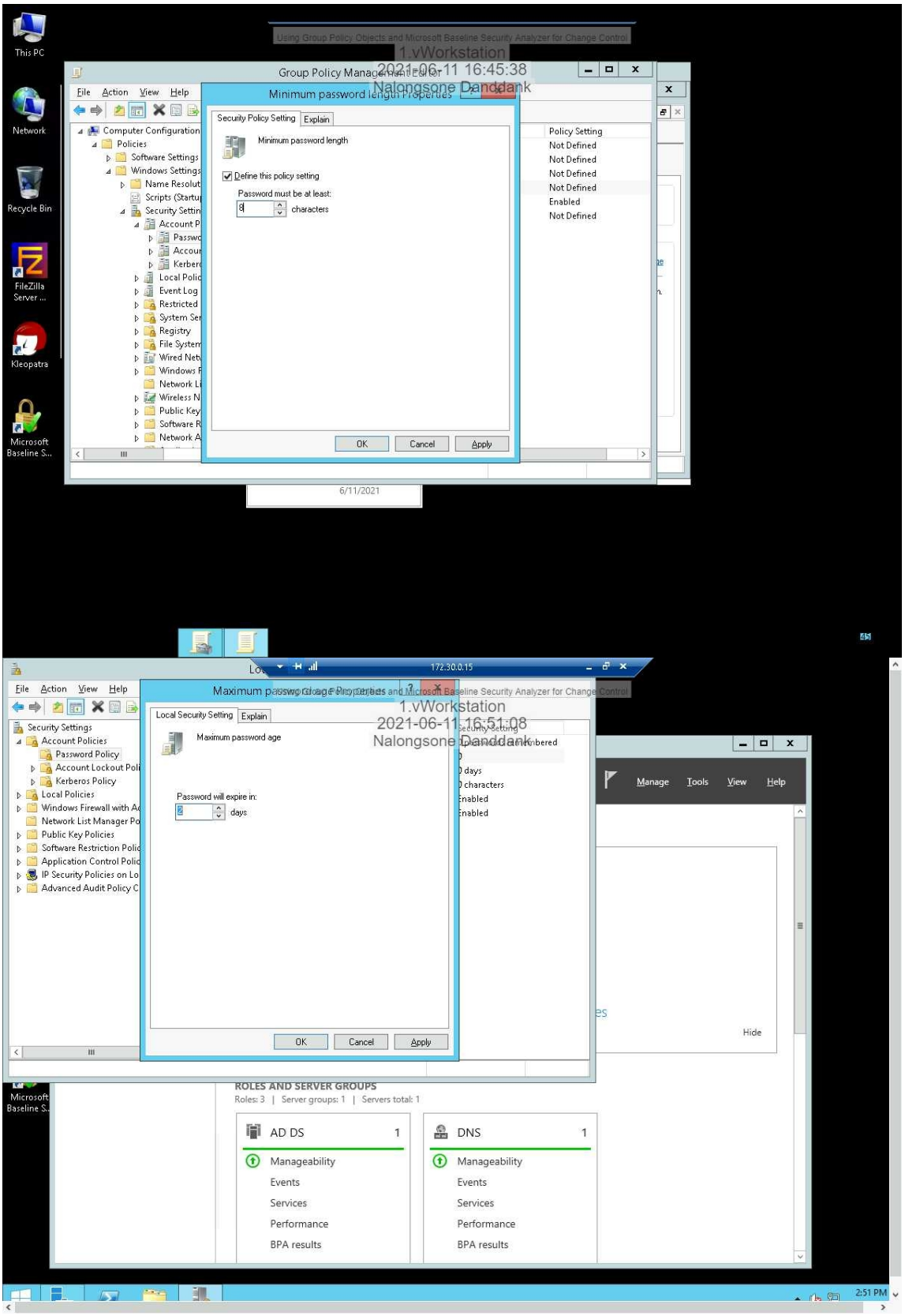

172.30.0.15
Group Policy Management
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:14:01
Nalongsone Danddank
File Action View Window Help
Group Policy Management
Forest: securelabsondemand.com
Contents
Name
Forest: securelabsondemand.com
Performance
BPA results
All Servers 1
Manageability
2:14 PM
6/11/2021

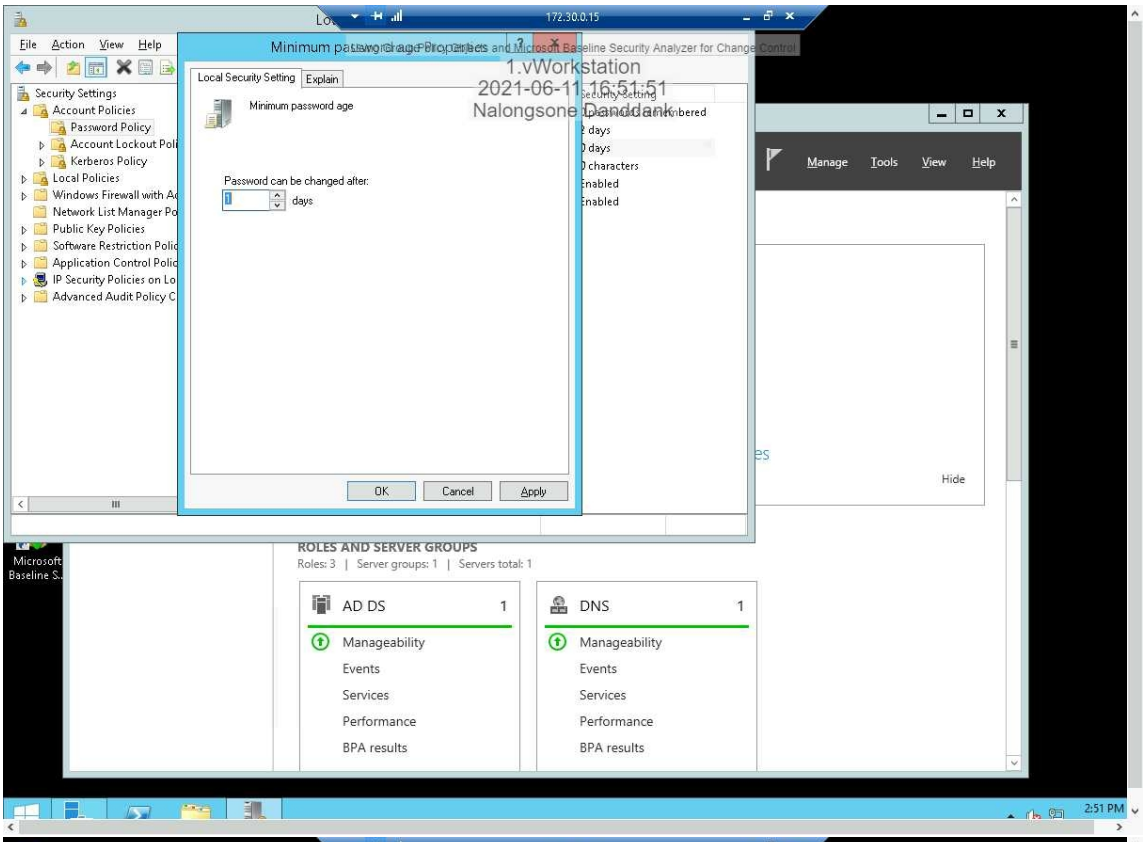

172.30.0.15
Group Policy Management
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:16:40
Nalongsone Danddank
File Action View Window Help
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Domain Controllers
WMI Filters
Starter GPOs
Sites
Group Policy Modelin
Group Policy Results
Group Policy Objects in securelabsondemand
Contents
Delegation
Name
GPO Status
Default Domain Controllers Policy
Enabled
Enabled
New GPO
Name:
New Group Policy Object
Source Starter GPO:
(none)
OK
Cancel
Performance
BPA results
All Servers 1
Manageability
2:16 PM
6/11/2021

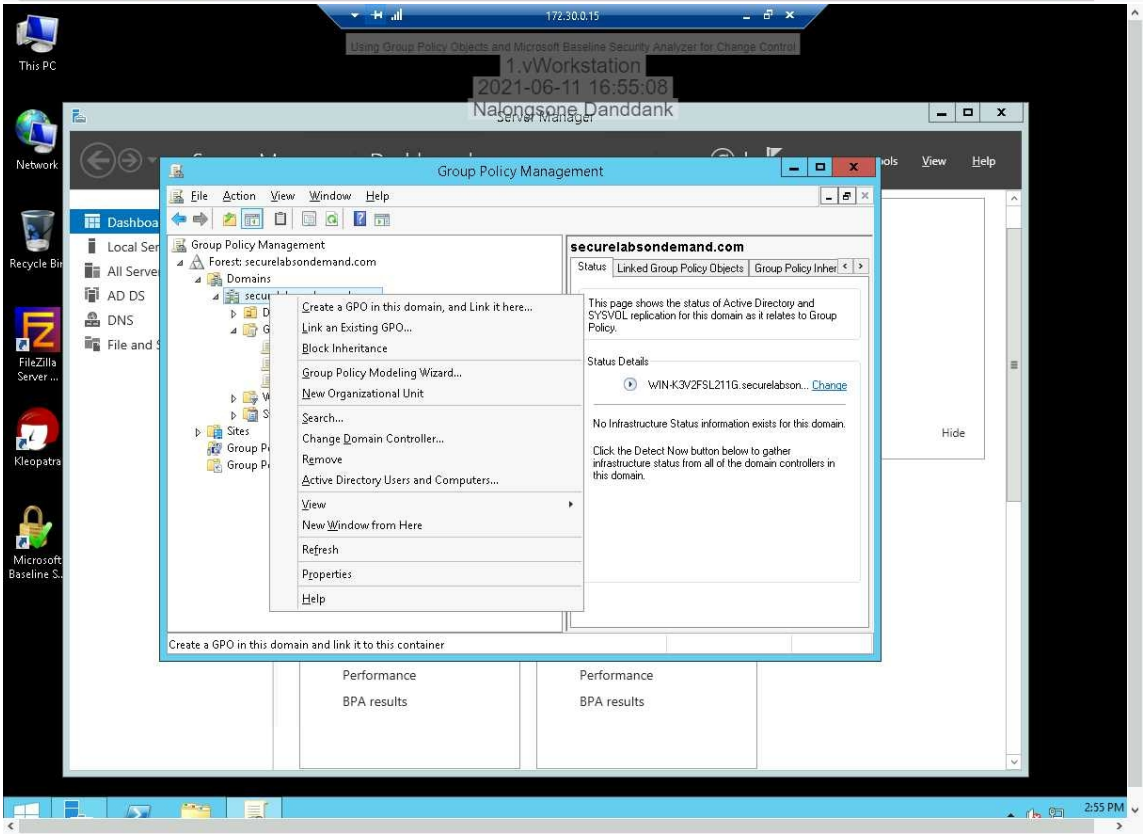

172.30.0.15
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
PasswordGPO
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
PasswordGPO
Scope Details Settings Delegation Status
Links
Display links in this location:
The following sites, domains, and OUs are linked to this GPO:
Location
Security Filtering
The settings in this GPO can only apply to the following groups,
Name
Authenticated Users
Add... Remove
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Performance
BPA results
Performance
BPA results
All Servers 1
Manageability
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:19:35
Nalongsone Danddank
2:19 PM
6/11/2021
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:40:07
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Public Key Policies
Software Restriction Policies
Network Access Protection
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
Not Defined
Password must meet complexity requirements
Not Defined
Store passwords using reversible encryption
Not Defined
6/11/2021

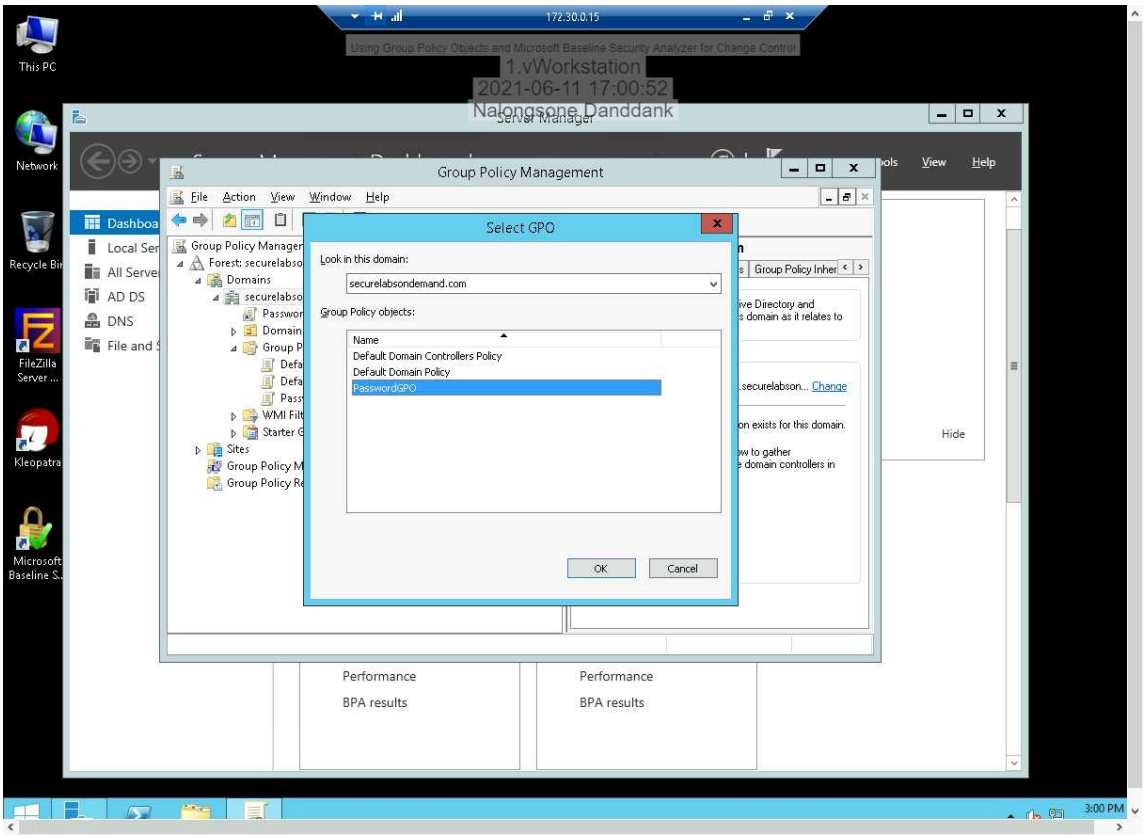

Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:41:48
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Password must meet complexity requirements Pro...
Security Policy Setting
Explain
Password must meet complexity requirements
This security setting determines whether passwords must meet complexity requirements.
If this policy is enabled, passwords must meet the following minimum requirements:
Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least six characters in length
Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.
Default:
Enabled on domain controllers.
For more information about security policy and related Windows features, see the Microsoft website.
OK
Cancel
Apply
Policy Setting
Not Defined
6/11/2021
This PC
Network
Recycle Bin
FileZilla Server ...
Kleopatra
Microsoft Baseline S...

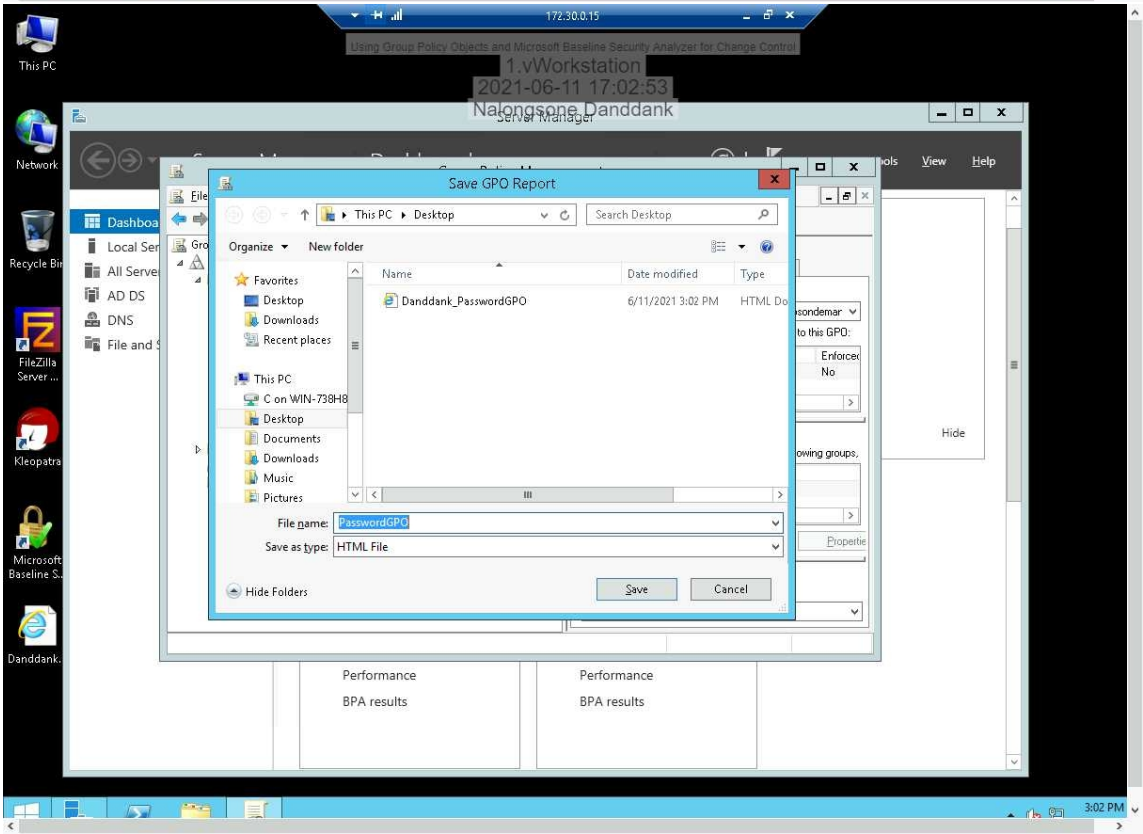

Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:43:22
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Password must meet complexity requirements Pro...
Security Policy Setting
Explain
Password must meet complexity requirements
Define this policy setting:
Enabled
Disabled
OK
Cancel
Apply
Policy Setting
Not Defined
6/11/2021
This PC
Network
Recycle Bin
FileZilla Server ...
Kleopatra
Microsoft Baseline S...

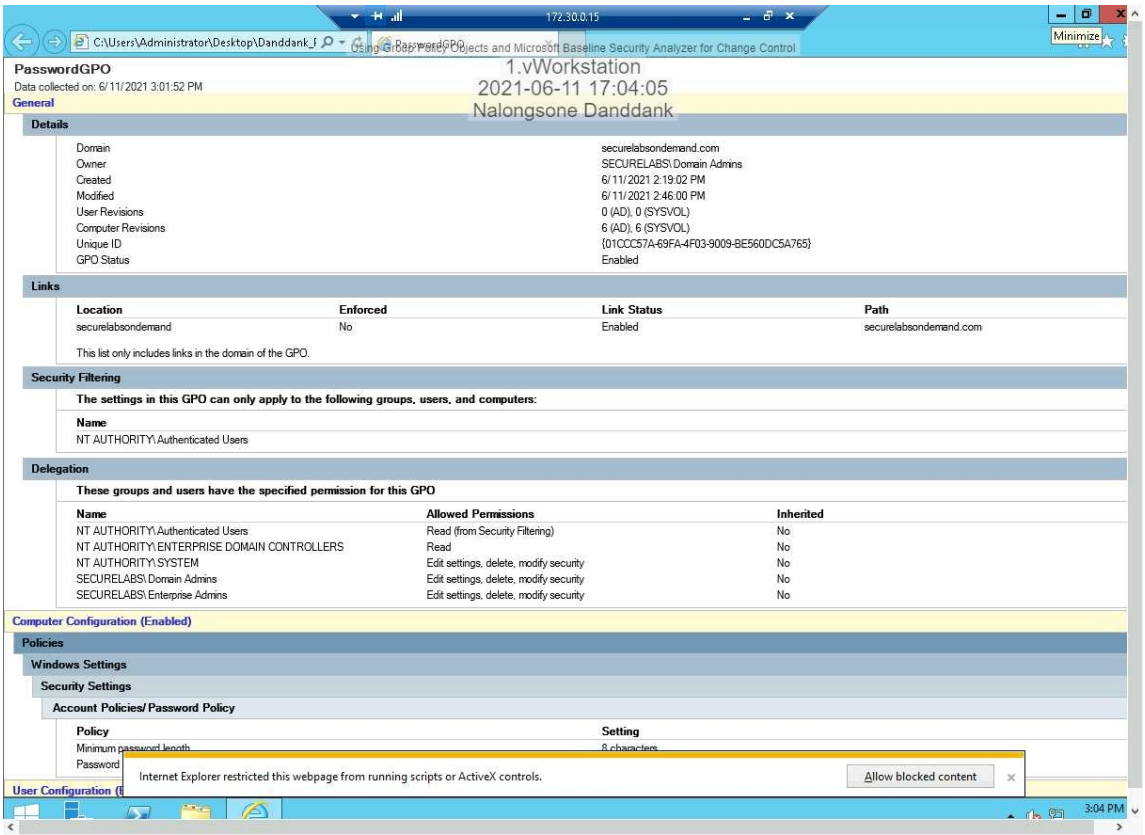

Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:45:38
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Minimum password length Properties
Security Policy Setting Explain
Minimum password length
Define this policy setting
Password must be at least:
8
characters
OK Cancel Apply
Policy Setting
Not Defined
Not Defined
Not Defined
Not Defined
Enabled
Not Defined
6/11/2021
172.30.0.15
Maximum password age Properties
Local Security Setting Explain
Maximum password age
Password will expire in:
42
days
1.vWorkstation
2021-06-11 16:51:08
Nalongsone Danddank
Manage Tools View Help
Hide
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS 1
Manageability
Events
Services
Performance
BPA results
2:51 PM

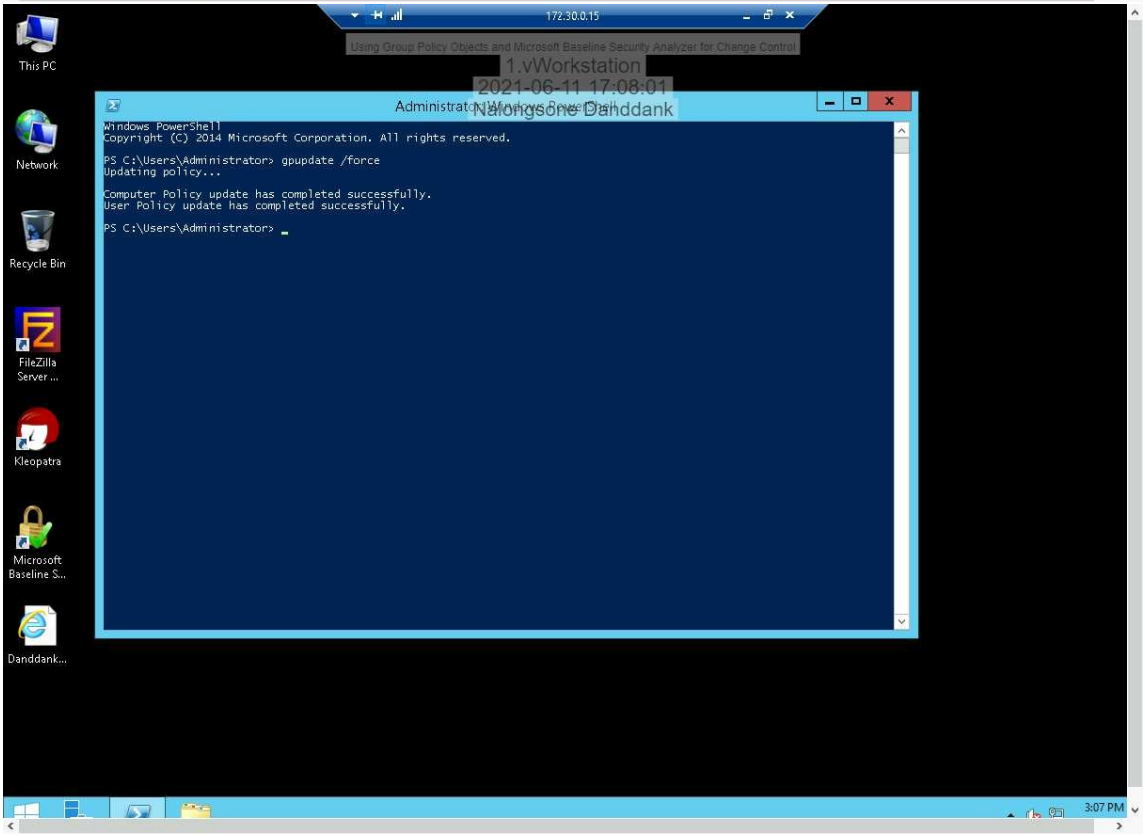

172.30.0.15
1.vWorkstation
2021-06-11 16:51:51
Nalongsone Danddank
Minimum password age Properties
Local Security Setting
Explain
Minimum password age
Password can be changed after:
days
OK
Cancel
Apply
Security Settings
Account Policies
Password Policy
Account Lockout Poli
Kerberos Policy
Local Policies
Windows Firewall with Ad
Network List Manager Po
Public Key Policies
Software Restriction Polic
Application Control Polic
IP Security Policies on Lo
Advanced Audit Policy C
Manage
Tools
View
Help
Hide
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS
1
Manageability
Events
Services
Performance
BPA results
DNS
1
Manageability
Events
Services
Performance
BPA results
2:51 PM


172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 16:55:08
Nalongsone Danddank
This PC
Network
Recycle Bin
FileZilla Server ...
Kleopatra
Microsoft Baseline S...
Server Manager
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: securelabsondemand.com
Domains
Sites
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help
securelabsondemand.com
Status
Linked Group Policy Objects
Group Policy Inher
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.
Status Details
WIN-K3V2FSL211G.securelabson... Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.
Create a GPO in this domain and link it to this container
Manage
Tools
View
Help
Hide
Performance
BPA results
Performance
BPA results
2:55 PM

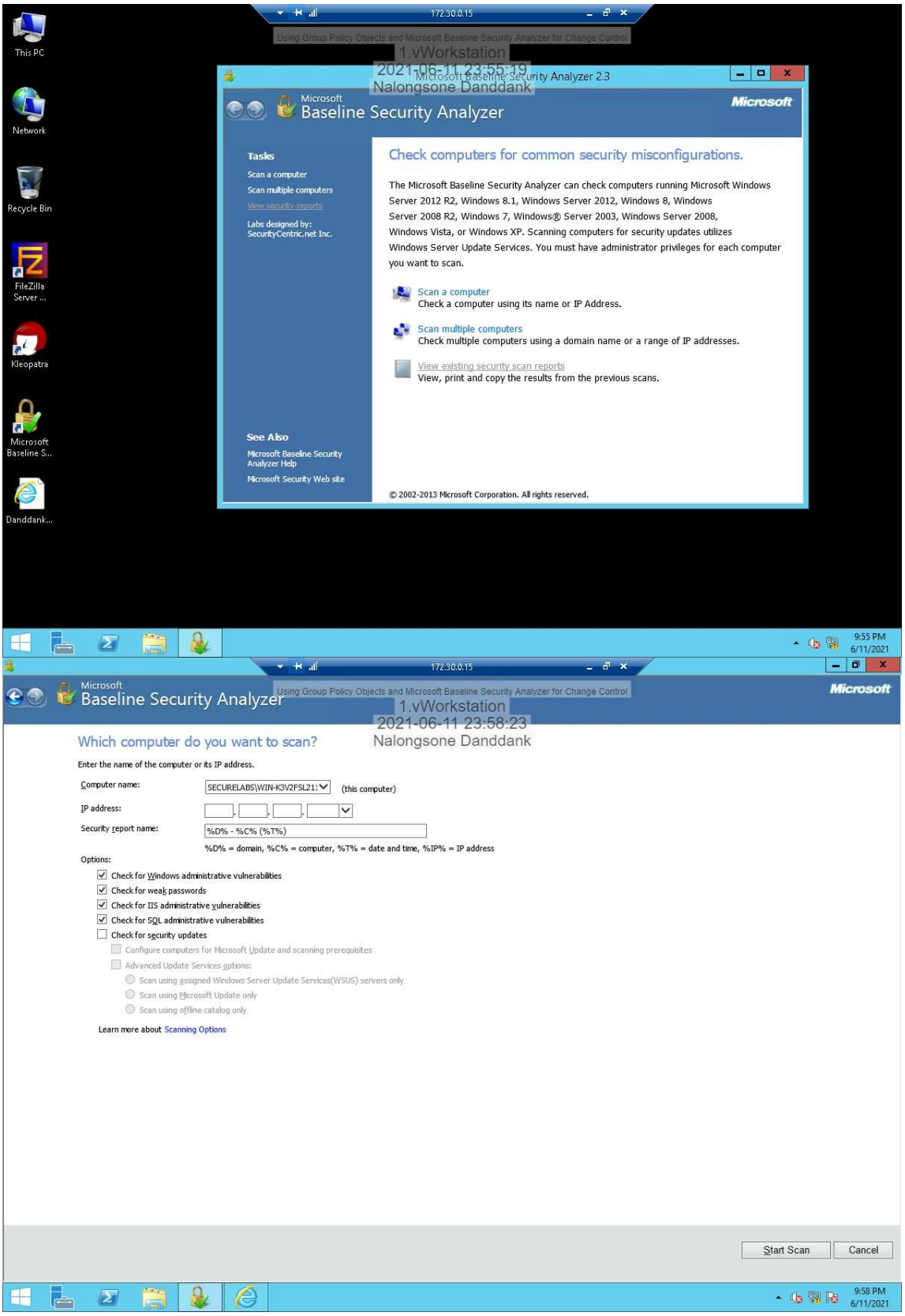

172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 17:00:52
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Select GPO
Look in this domain:
securelabsondemand.com
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
PasswordGPO
OK
Cancel
Performance
BPA results
Performance
BPA results
3:00 PM

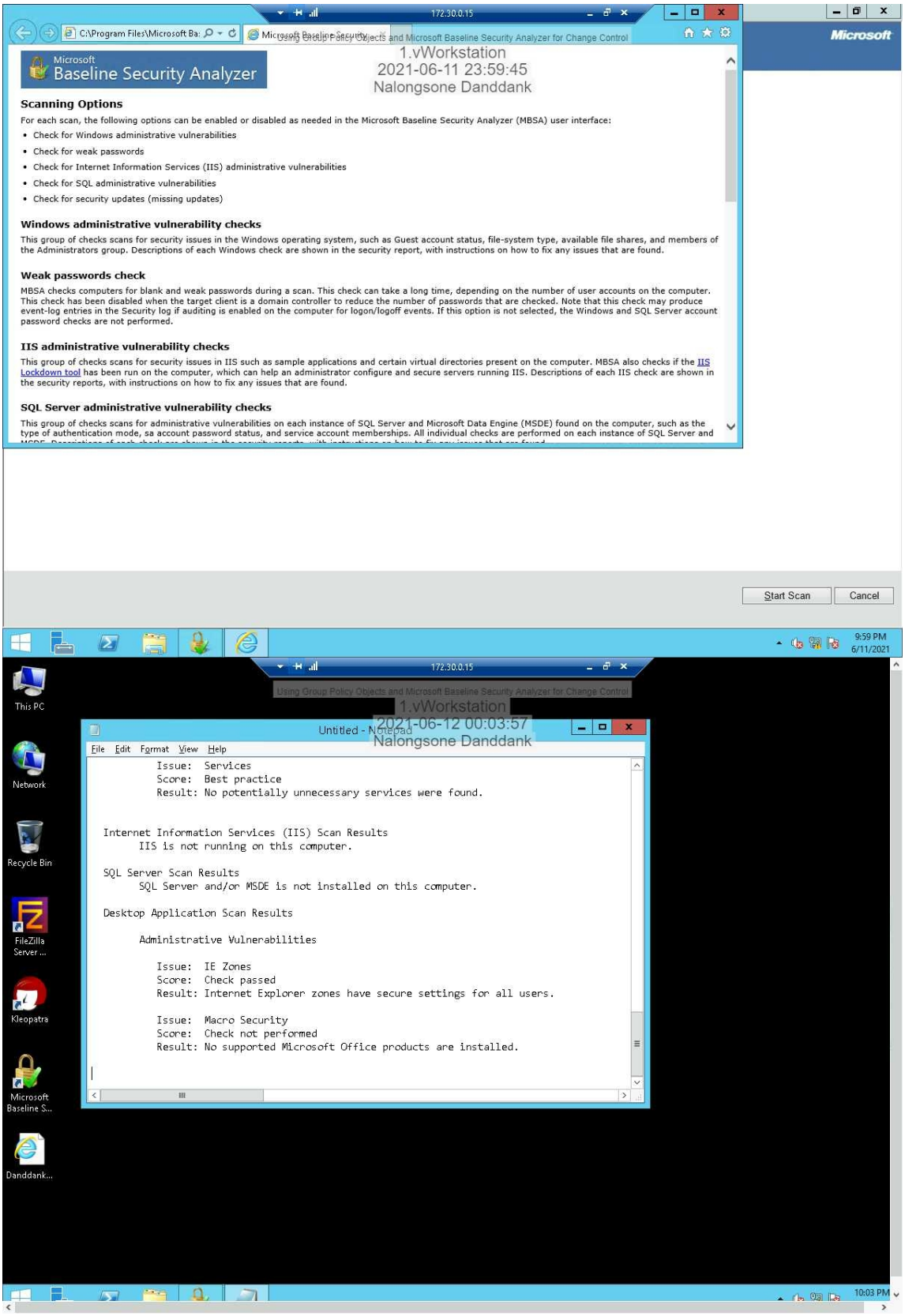

172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 17:02:53
Nalongsone Danddank
Save GPO Report
This PC ▸ Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent places
This PC
Documents
Music
Pictures
Name
Date modified
Type
Danddank_PasswordGPO
6/11/2021 3:02 PM
File name: PasswordGPO
Save as type: HTML File
Hide Folders
Save
Cancel
Performance
BPA results
Performance
BPA results
3:02 PM

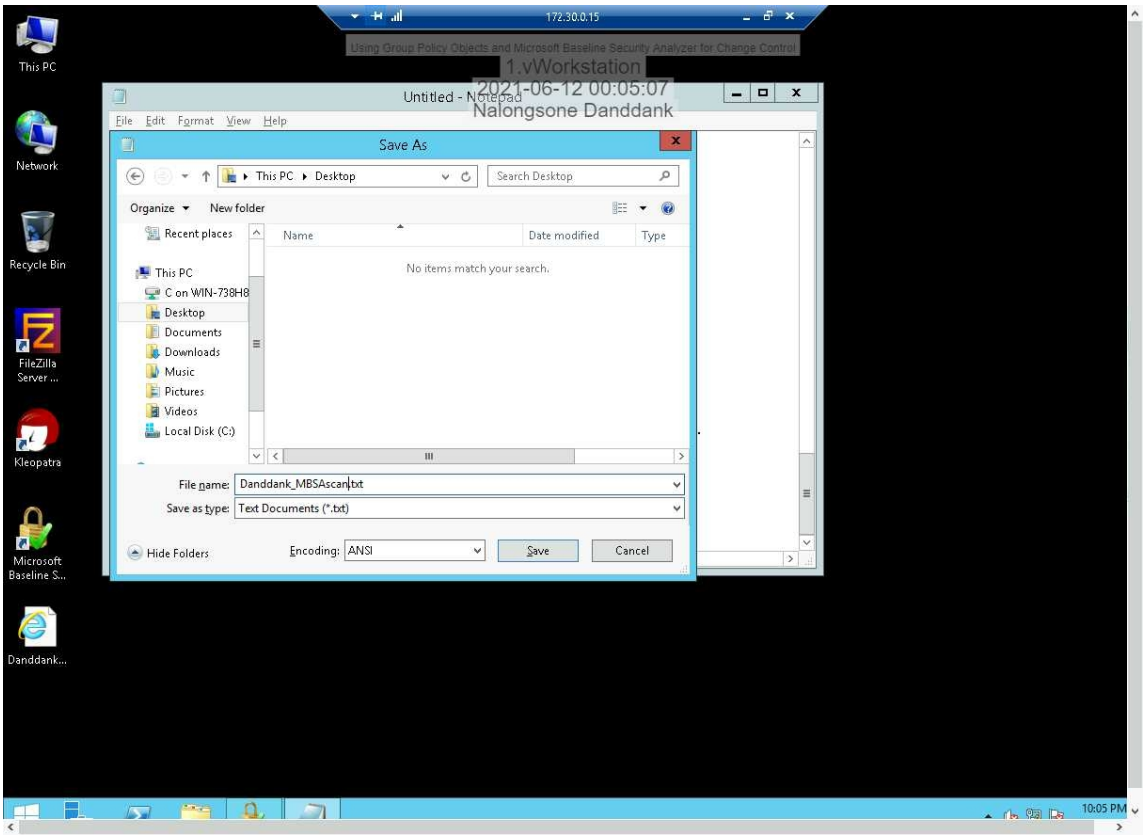


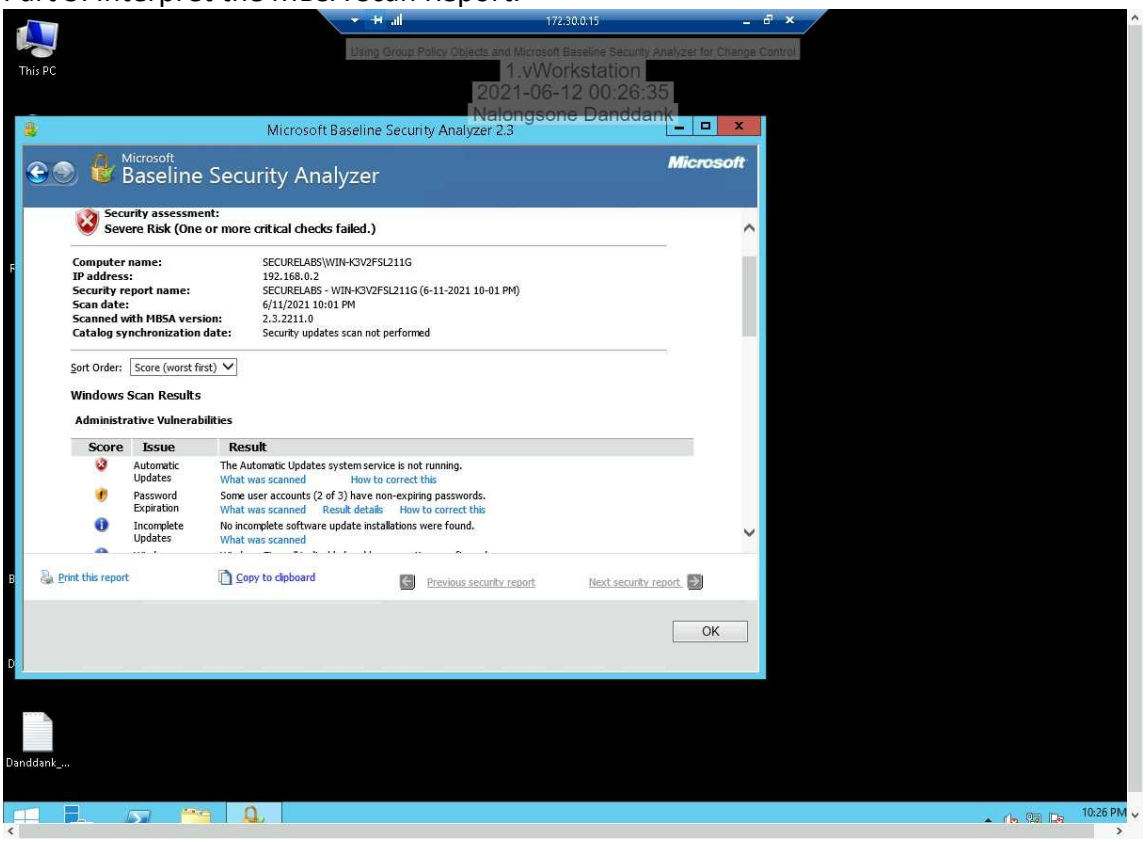

Part 2: Scan TargetWindowsDC01 with Microsoft Baseline Security Analyzer.

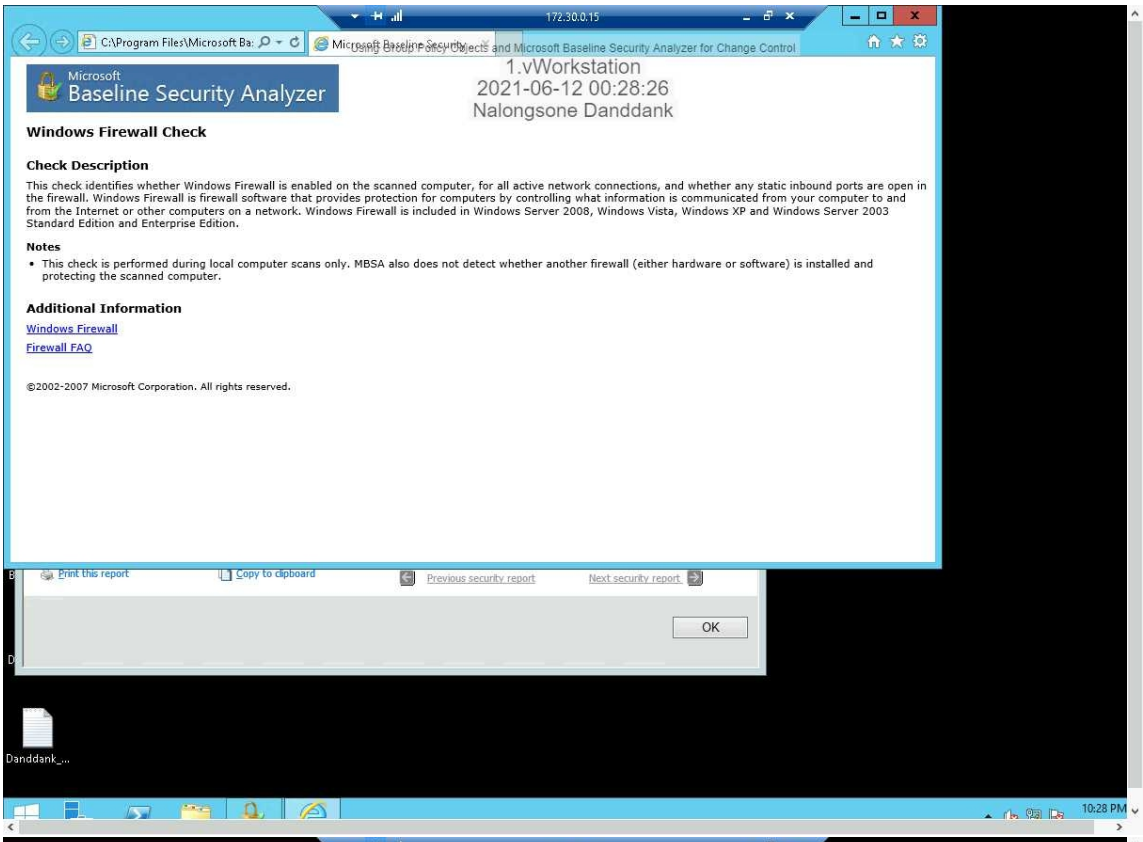

172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 23:55:19
Nalongsone Danddank
Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
Labs designed by:
SecurityCentric.net Inc.
Check computers for common security misconfigurations.
The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.
Scan a computer
Check a computer using its name or IP Address.
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.
View existing security scan reports
View, print and copy the results from the previous scans.
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site
© 2002-2013 Microsoft Corporation. All rights reserved.
This PC
Network
Recycle Bin
FileZilla Server ...
Kleopatra
Microsoft Baseline S...
Danddank...
9:55 PM
6/11/2021
172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 23:58:23
Nalongsone Danddank
Microsoft
Baseline Security Analyzer
Microsoft
Which computer do you want to scan?
Enter the name of the computer or its IP address.
Computer name:
SECURELABS\WIN-K3V2FSL21
(this computer)
IP address:
Security report name:
%D% - %C% (%T%)
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address
Options:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for IIS administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates
Configure computers for Microsoft Update and scanning prerequisites
Advanced Update Services options:
Scan using assigned Windows Server Update Services(WSUS) servers only
Scan using Microsoft Update only
Scan using offline catalog only
Learn more about Scanning Options
Start Scan
Cancel
9:58 PM
6/11/2021

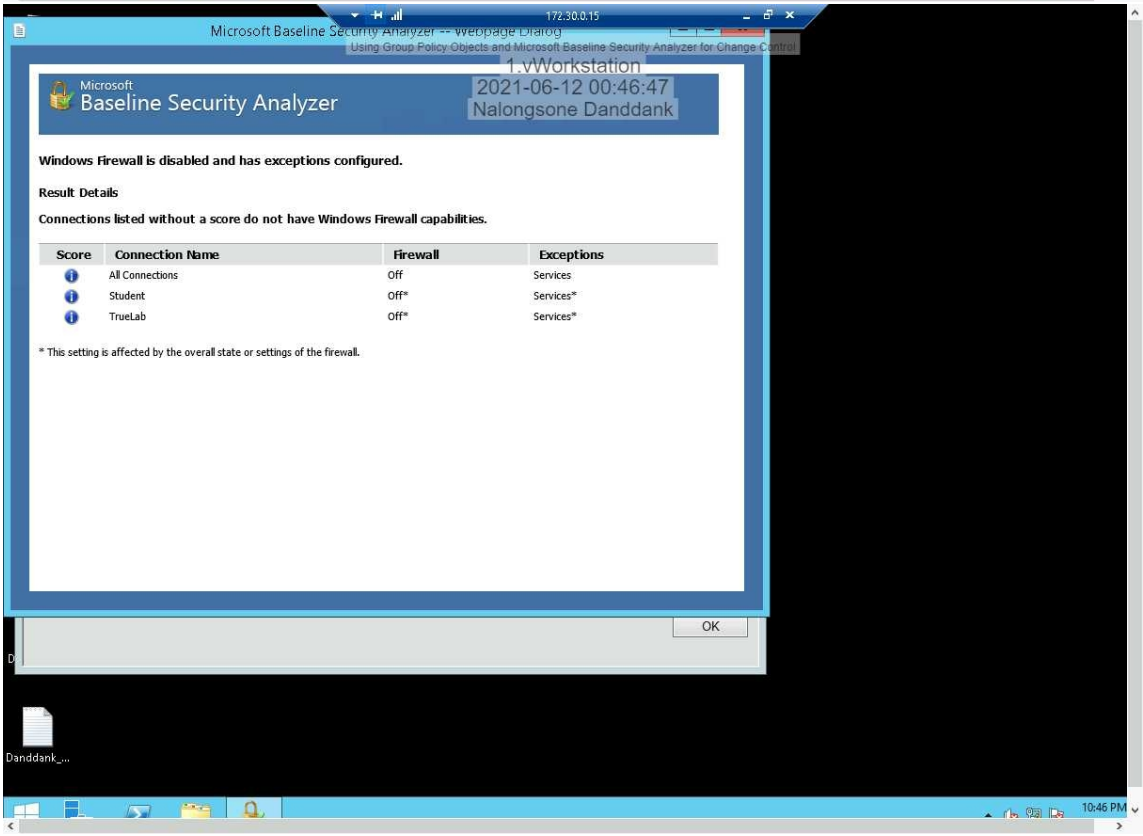

172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-11 23:59:45
Nalongsone Danddank
Microsoft Baseline Security Analyzer
Scanning Options
For each scan, the following options can be enabled or disabled as needed in the Microsoft Baseline Security Analyzer (MBSA) user interface:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for Internet Information Services (IIS) administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates (missing updates)
Windows administrative vulnerability checks
This group of checks scans for security issues in the Windows operating system, such as Guest account status, file-system type, available file shares, and members of the Administrators group. Descriptions of each Windows check are shown in the security report, with instructions on how to fix any issues that are found.
Weak passwords check
MBSA checks computers for blank and weak passwords during a scan. This check can take a long time, depending on the number of user accounts on the computer. This check has been disabled when the target client is a domain controller to reduce the number of passwords that are checked. Note that this check may produce event-log entries in the Security log if auditing is enabled on the computer for logon/logoff events. If this option is not selected, the Windows and SQL Server account password checks are not performed.
IIS administrative vulnerability checks
This group of checks scans for security issues in IIS such as sample applications and certain virtual directories present on the computer. MBSA also checks if the IIS Lockdown tool has been run on the computer, which can help an administrator configure and secure servers running IIS. Descriptions of each IIS check are shown in the security reports, with instructions on how to fix any issues that are found.
SQL Server administrative vulnerability checks
This group of checks scans for administrative vulnerabilities on each instance of SQL Server and Microsoft Data Engine (MSDE) found on the computer, such as the type of authentication mode, sa account password status, and service account memberships. All individual checks are performed on each instance of SQL Server and
Start Scan
Cancel
9:59 PM
6/11/2021
172.30.0.15
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-12 00:03:57
Nalongsone Danddank
Untitled - Notepad
File Edit Format View Help
Issue: Services
Score: Best practice
Result: No potentially unnecessary services were found.
Internet Information Services (IIS) Scan Results
IIS is not running on this computer.
SQL Server Scan Results
SQL Server and/or MSDE is not installed on this computer.
Desktop Application Scan Results
Administrative Vulnerabilities
Issue: IE Zones
Score: Check passed
Result: Internet Explorer zones have secure settings for all users.
Issue: Macro Security
Score: Check not performed
Result: No supported Microsoft Office products are installed.
This PC
Network
Recycle Bin
FileZilla Server ...
Kleopatra
Microsoft Baseline S...
Danddank...
10:03 PM

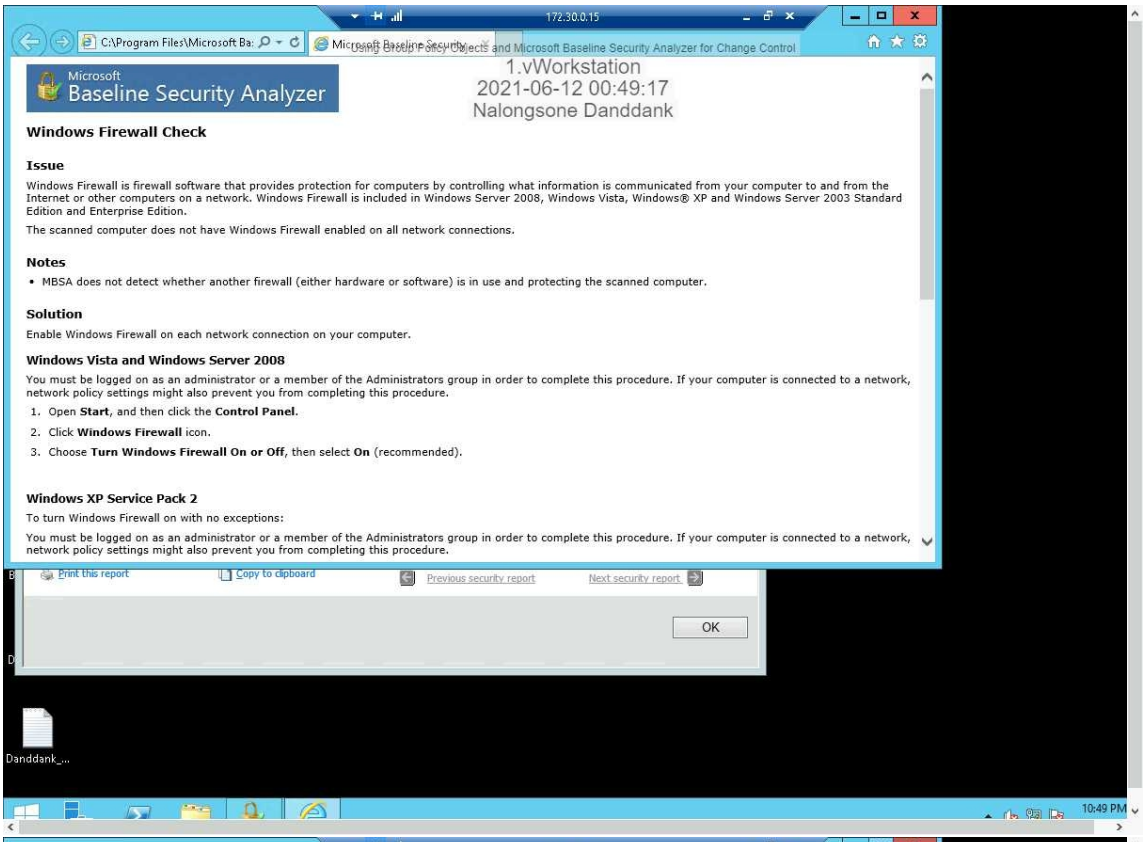


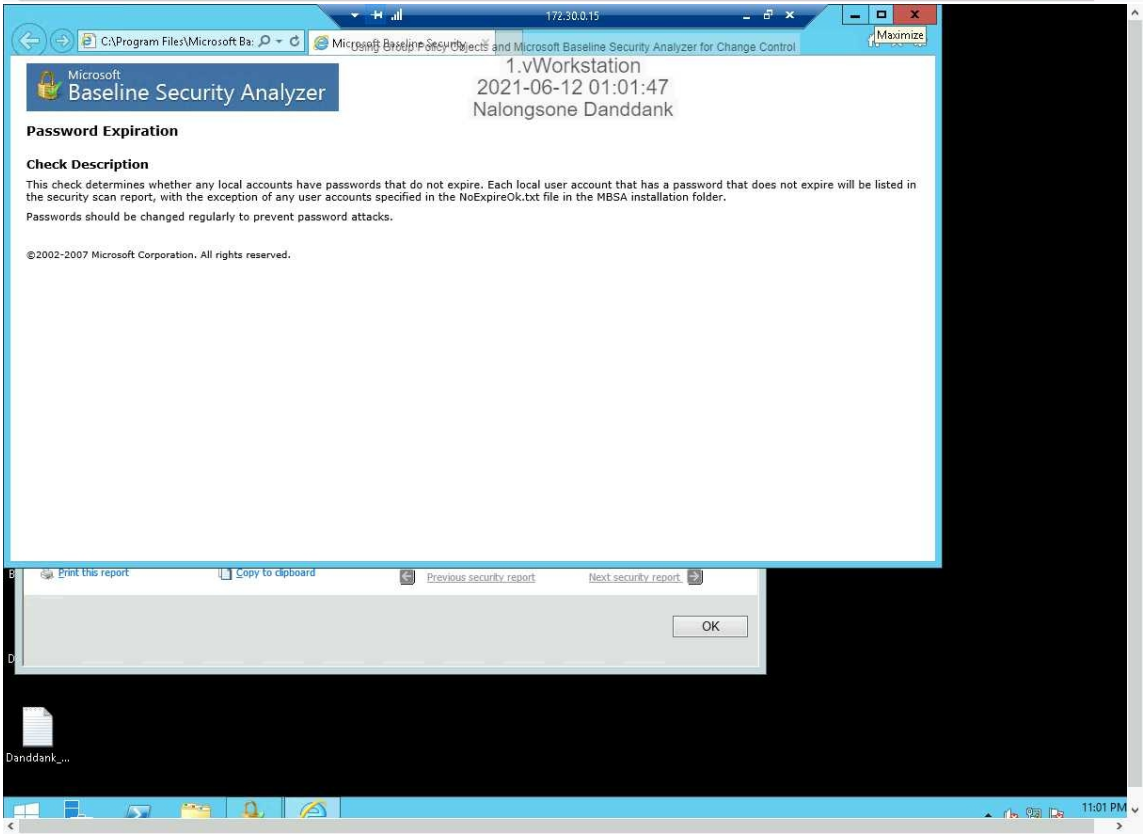

Part 3: Interpret the MBSA Scan Report.

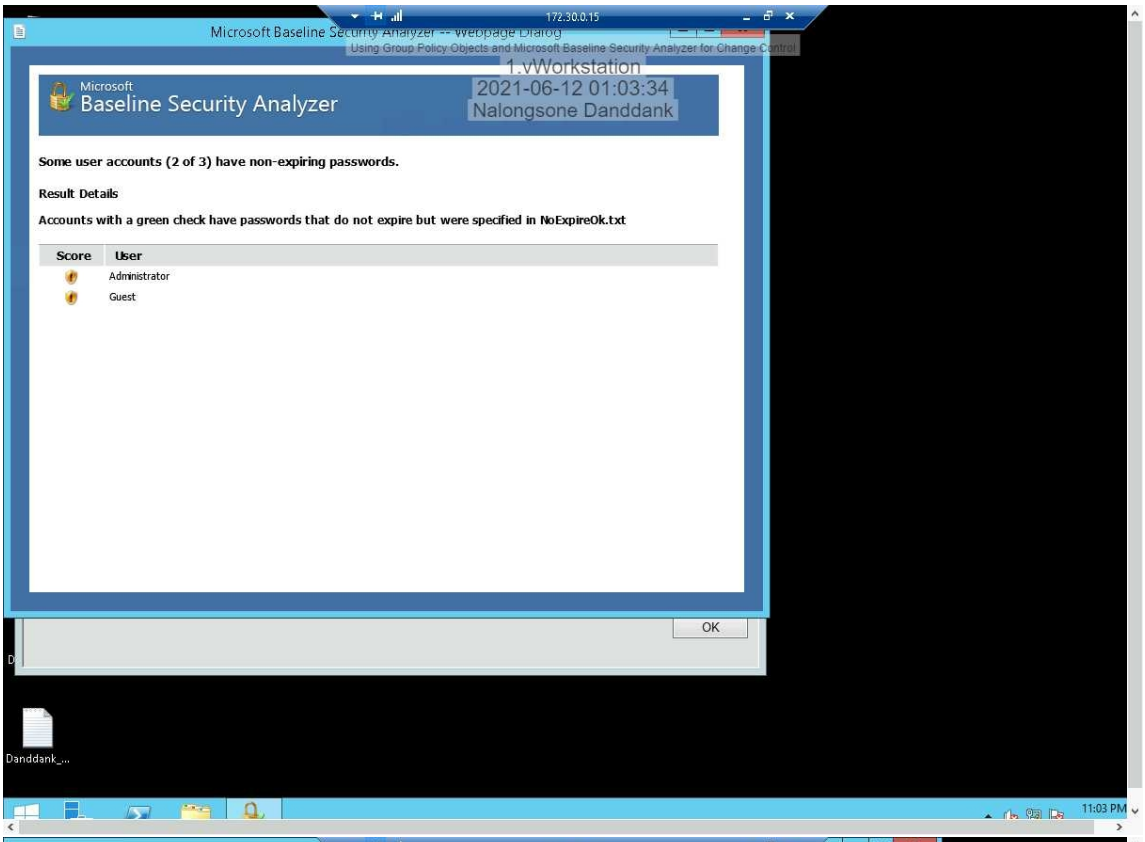


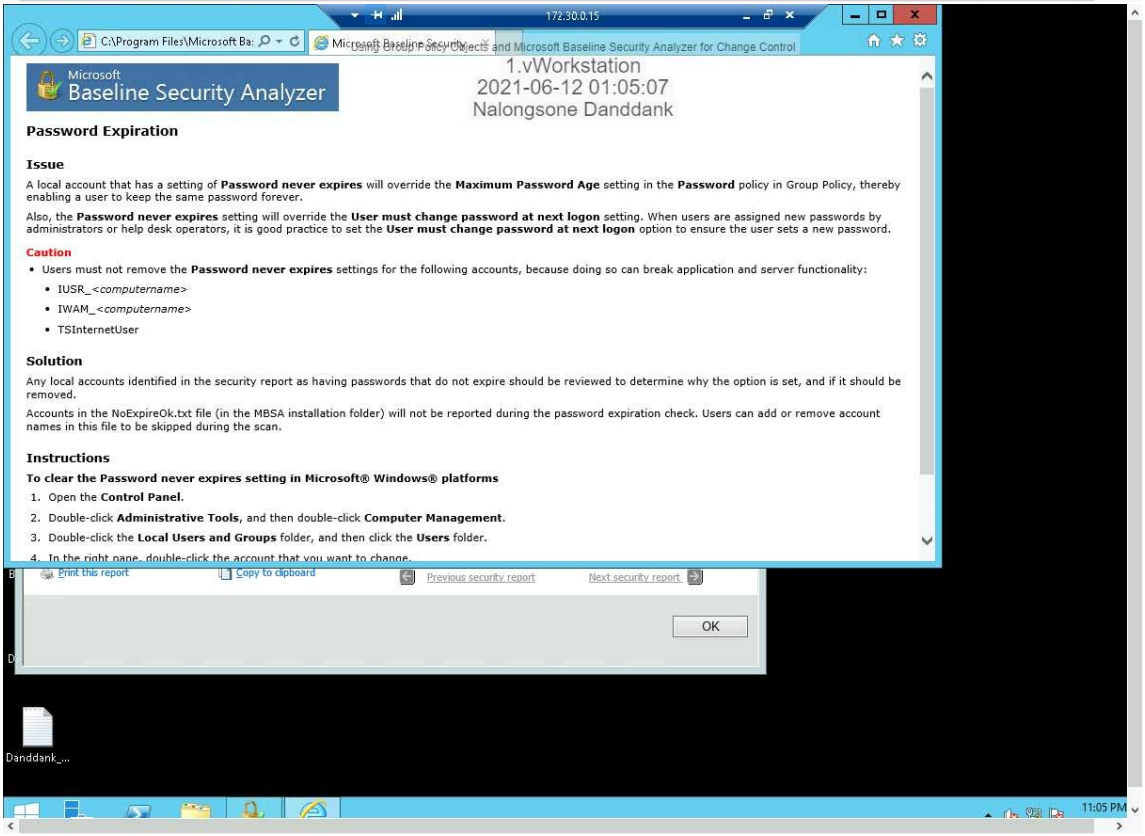

172.30.0.15
C:\Program Files\Microsoft Ba:
Microsoft Baseline Security
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
Microsoft
Baseline Security Analyzer
1.vWorkstation
2021-06-12 00:28:26
Nalongsone Danddank
Windows Firewall Check
Check Description
This check identifies whether Windows Firewall is enabled on the scanned computer, for all active network connections, and whether any static inbound ports are open in the firewall. Windows Firewall is firewall software that provides protection for computers by controlling what information is communicated from your computer to and from the Internet or other computers on a network. Windows Firewall is included in Windows Server 2008, Windows Vista, Windows XP and Windows Server 2003 Standard Edition and Enterprise Edition.
Notes
• This check is performed during local computer scans only. MBSA also does not detect whether another firewall (either hardware or software) is installed and protecting the scanned computer.
Additional Information
Windows Firewall
Firewall FAQ
©2002-2007 Microsoft Corporation. All rights reserved.
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Danddank_...
10:28 PM


172.30.0.15
Microsoft Baseline Security Analyzer -- Webpage Dialog
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
Microsoft
Baseline Security Analyzer
2021-06-12 00:46:47
Nalongsone Danddank
Windows Firewall is disabled and has exceptions configured.
Result Details
Connections listed without a score do not have Windows Firewall capabilities.
Score
Connection Name
Firewall
Exceptions
All Connections
Off
Services
Student
Off*
Services*
TrueLab
Off*
Services*
* This setting is affected by the overall state or settings of the firewall.
OK
Danddank_...
10:46 PM


172.30.0.15
C:\Program Files\Microsoft Ba:
Microsoft Baseline Security
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
Microsoft
Baseline Security Analyzer
1.vWorkstation
2021-06-12 00:49:17
Nalongsone Danddank
Windows Firewall Check
Issue
Windows Firewall is firewall software that provides protection for computers by controlling what information is communicated from your computer to and from the Internet or other computers on a network. Windows Firewall is included in Windows Server 2008, Windows Vista, Windows® XP and Windows Server 2003 Standard Edition and Enterprise Edition.
The scanned computer does not have Windows Firewall enabled on all network connections.
Notes
• MBSA does not detect whether another firewall (either hardware or software) is in use and protecting the scanned computer.
Solution
Enable Windows Firewall on each network connection on your computer.
Windows Vista and Windows Server 2008
You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.
1. Open Start, and then click the Control Panel.
2. Click Windows Firewall icon.
3. Choose Turn Windows Firewall On or Off, then select On (recommended).
Windows XP Service Pack 2
To turn Windows Firewall on with no exceptions:
You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Danddank_...
10:49 PM


172.30.0.15
C:\Program Files\Microsoft Ba:
Microsoft Baseline Security
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
Maximize
Microsoft
Baseline Security Analyzer
1.vWorkstation
2021-06-12 01:01:47
Nalongsone Danddank
Password Expiration
Check Description
This check determines whether any local accounts have passwords that do not expire. Each local user account that has a password that does not expire will be listed in the security scan report, with the exception of any user accounts specified in the NoExpireOk.txt file in the MBSA installation folder.
Passwords should be changed regularly to prevent password attacks.
©2002-2007 Microsoft Corporation. All rights reserved.
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Danddank_...
11:01 PM


172.30.0.15
Microsoft Baseline Security Analyzer -- Webpage Dialog
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-12 01:03:34
Nalongsone Danddank
Microsoft
Baseline Security Analyzer
Some user accounts (2 of 3) have non-expiring passwords.
Result Details
Accounts with a green check have passwords that do not expire but were specified in NoExpireOk.txt
Score
User
Administrator
Guest
OK
Danddank_...
11:03 PM


172.30.0.15
C:\Program Files\Microsoft Ba:
Microsoft Baseline Security
Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
1.vWorkstation
2021-06-12 01:05:07
Nalongsone Danddank
Microsoft
Baseline Security Analyzer
Password Expiration
Issue
A local account that has a setting of Password never expires will override the Maximum Password Age setting in the Password policy in Group Policy, thereby enabling a user to keep the same password forever.
Also, the Password never expires setting will override the User must change password at next logon setting. When users are assigned new passwords by administrators or help desk operators, it is good practice to set the User must change password at next logon option to ensure the user sets a new password.
Caution
Users must not remove the Password never expires settings for the following accounts, because doing so can break application and server functionality:
IUSR_<computername>
IWAM_<computername>
TSInternetUser
Solution
Any local accounts identified in the security report as having passwords that do not expire should be reviewed to determine why the option is set, and if it should be removed.
Accounts in the NoExpireOk.txt file (in the MBSA installation folder) will not be reported during the password expiration check. Users can add or remove account names in this file to be skipped during the scan.
Instructions
To clear the Password never expires setting in Microsoft® Windows® platforms
1. Open the Control Panel.
2. Double-click Administrative Tools, and then double-click Computer Management.
3. Double-click the Local Users and Groups folder, and then click the Users folder.
4. In the right pane, double-click the account that you want to change.
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Danddank_...
11:05 PM

End.