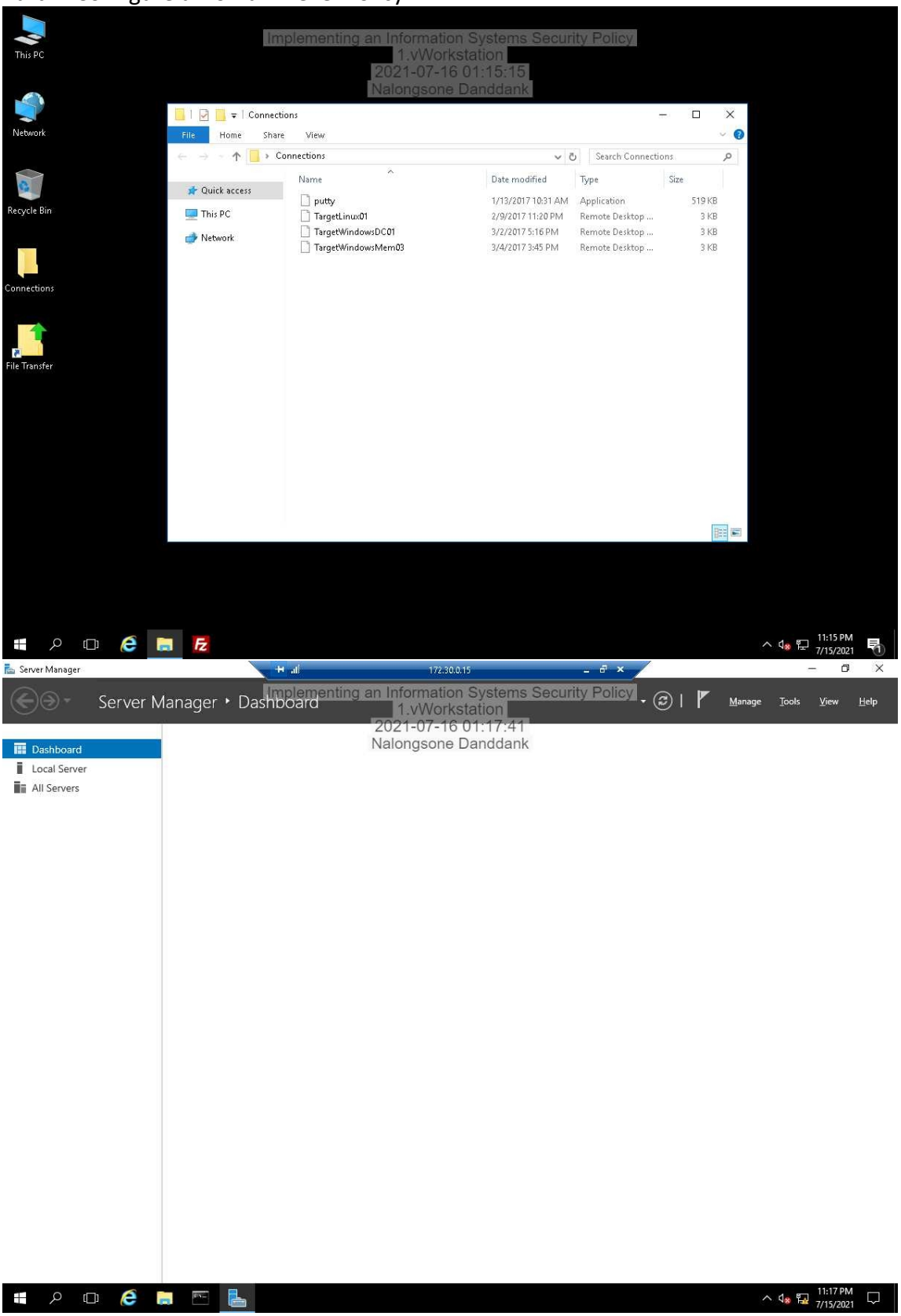
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

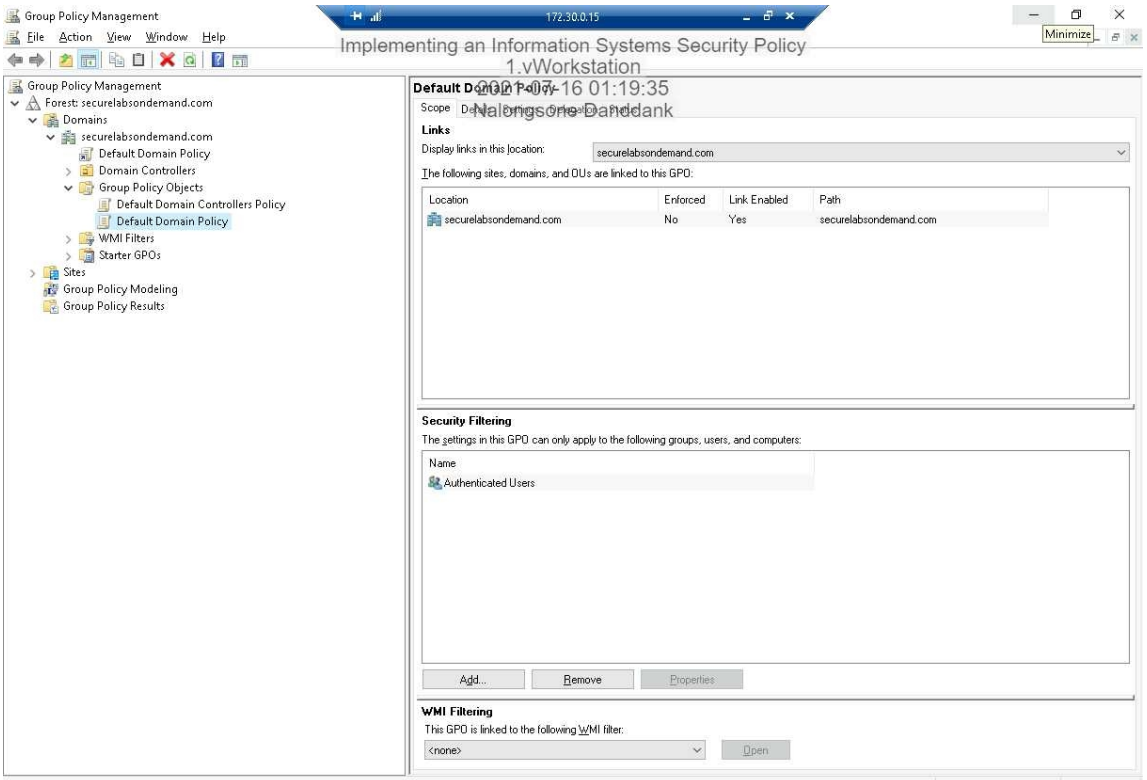
ICS382/CYBR332-51 —Computer Security

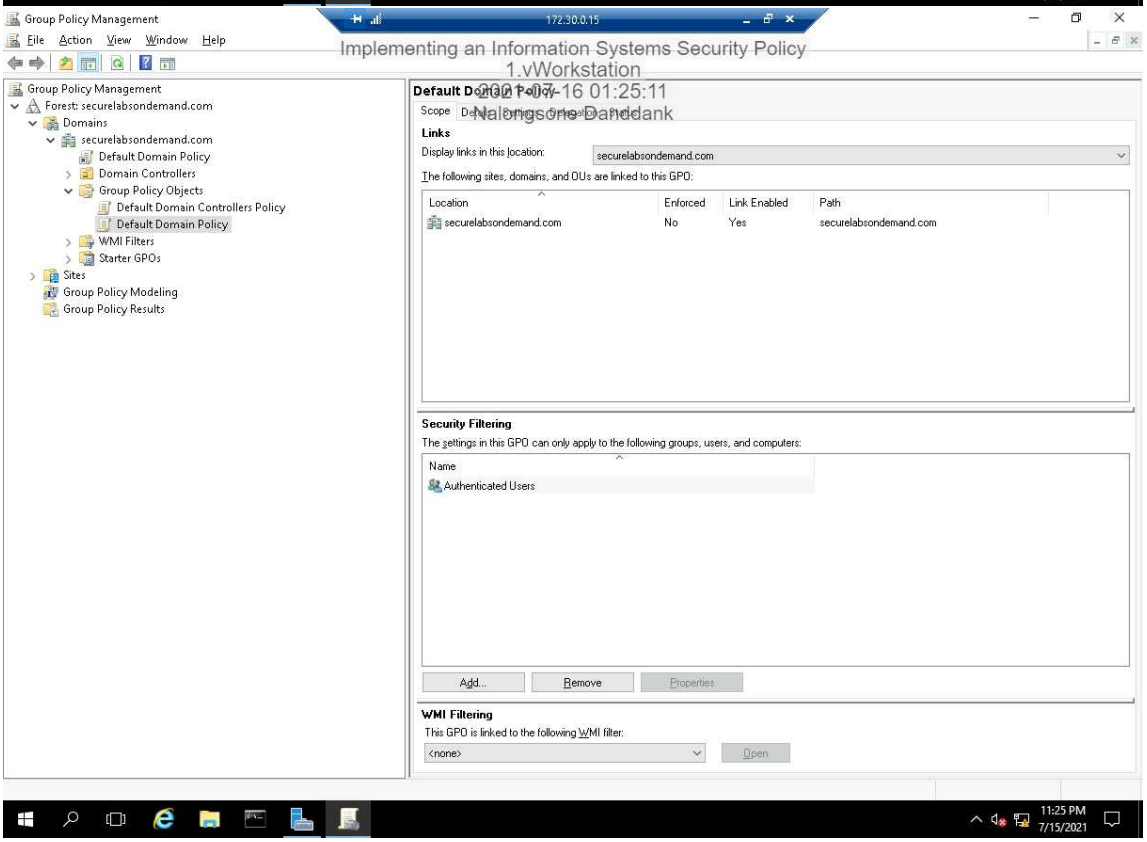
Lab #10 Report

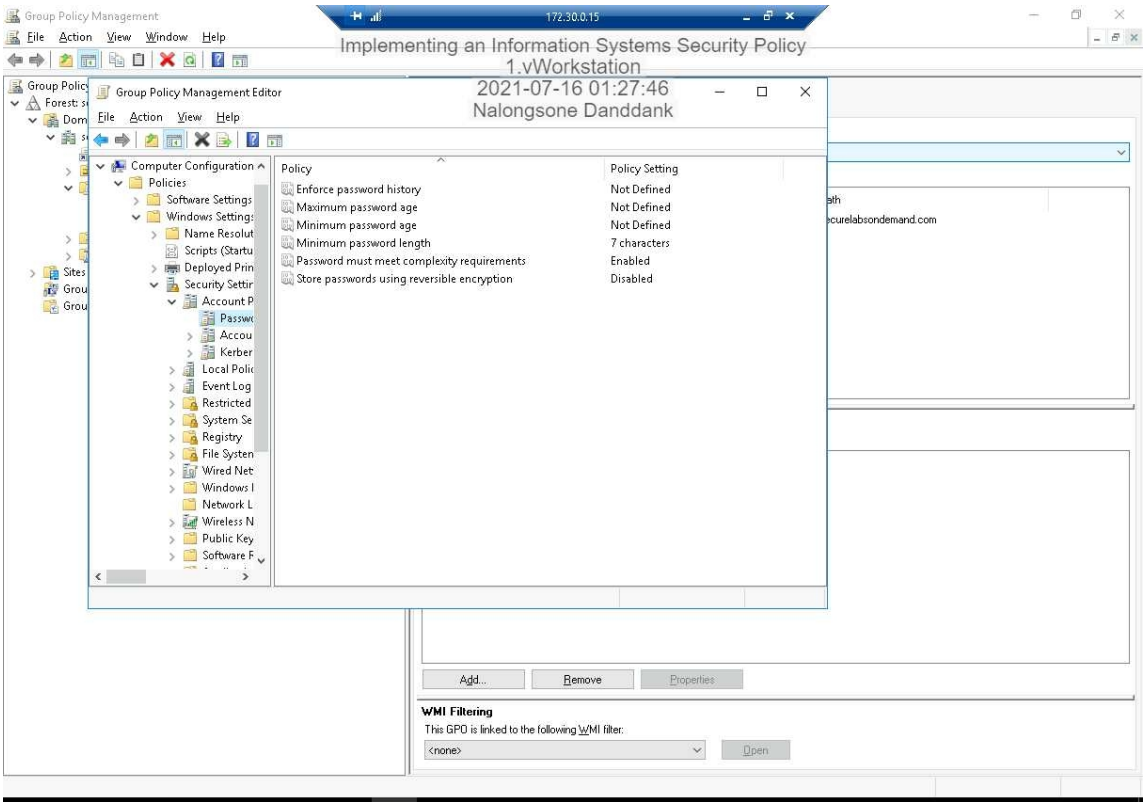
IMPLEMENTING AN INFORMATION SYSTEMS SECURITY POLICY

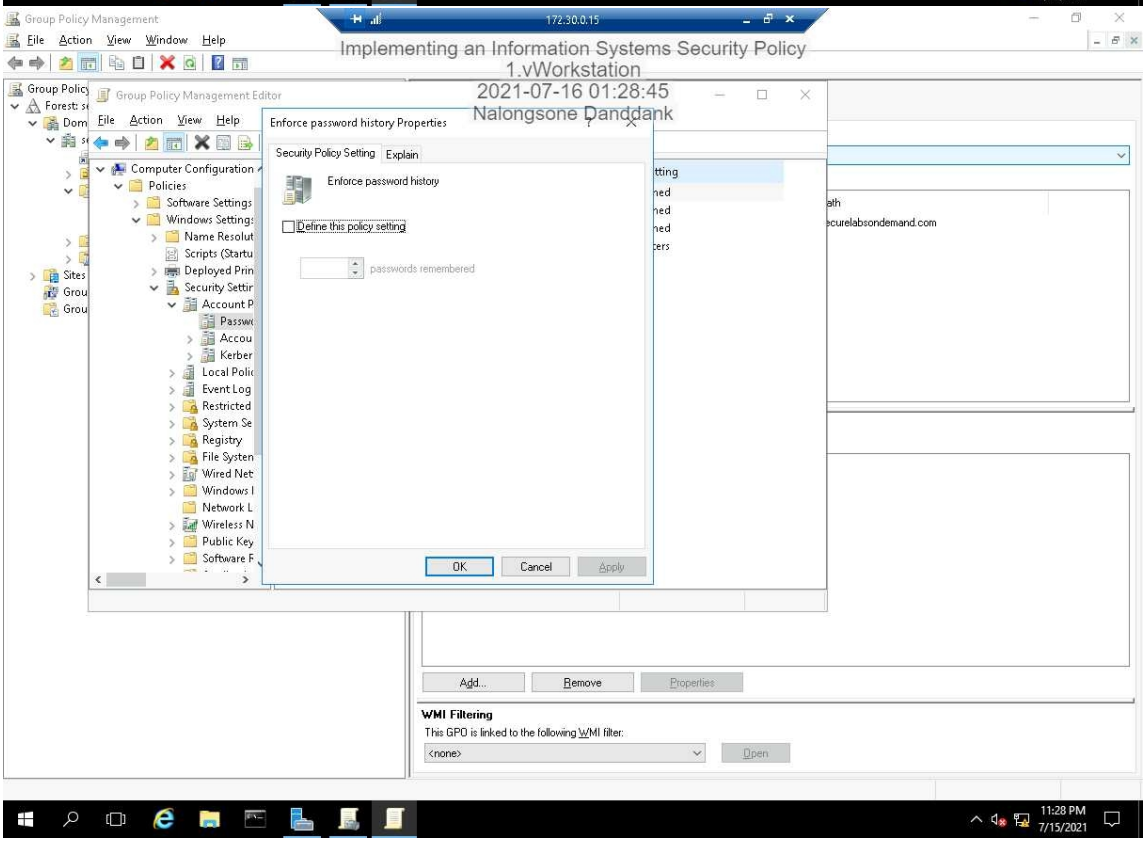
Part 1: Configure a Domain-Level Policy.

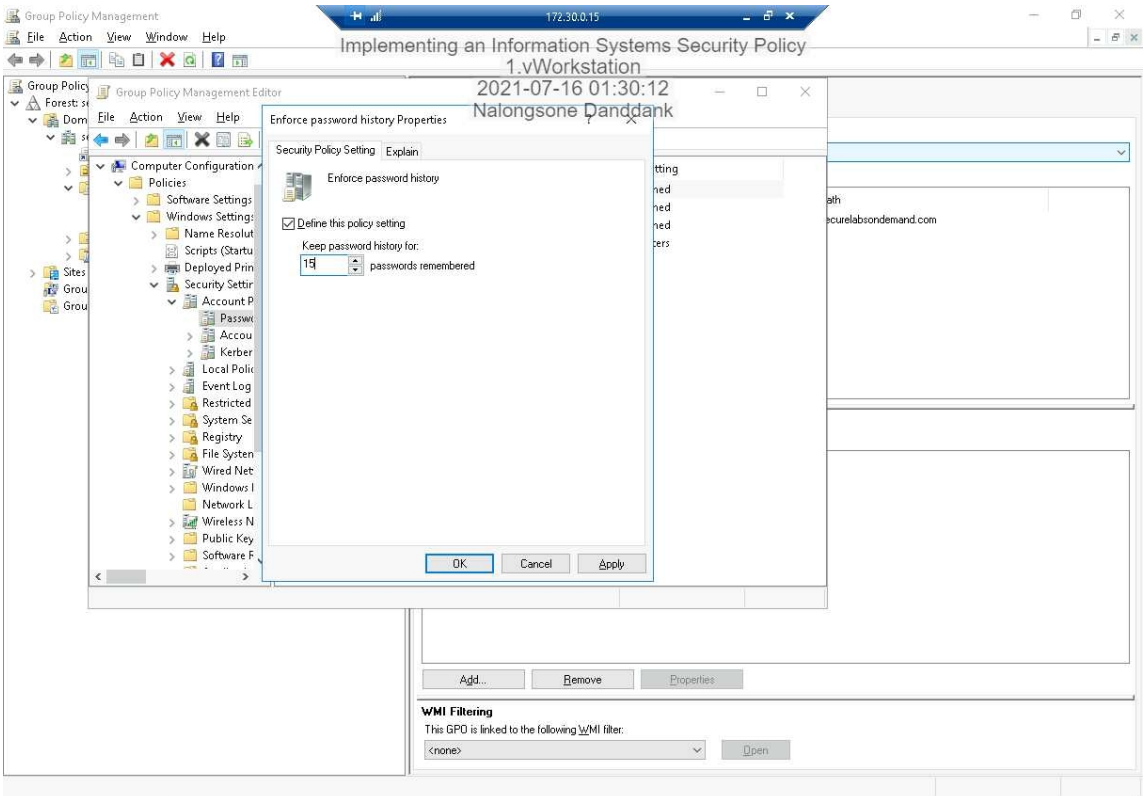


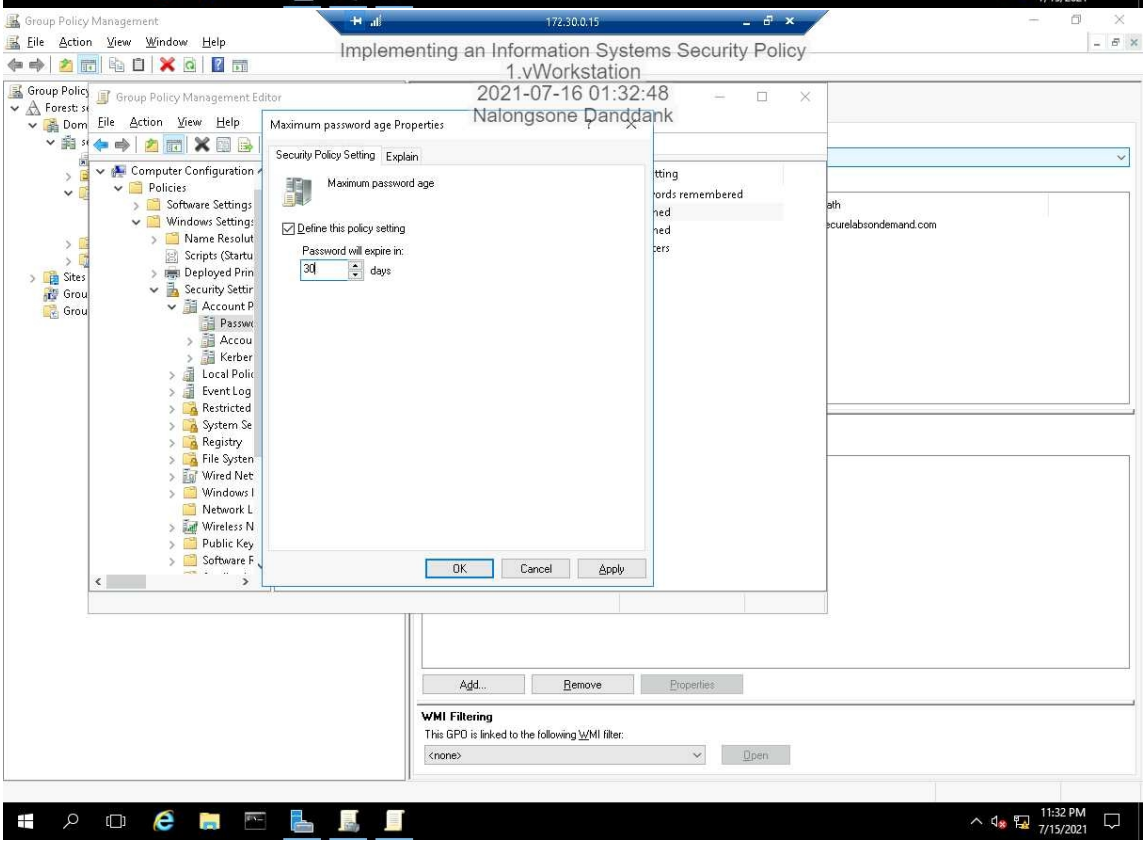

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:19:35
Nalongsone Danddank
Minimize
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Scope
Links
Display links in this location:
securelabsondemand.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
securelabsondemand.com
No
Yes
securelabsondemand.com
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:19 PM
7/15/2021

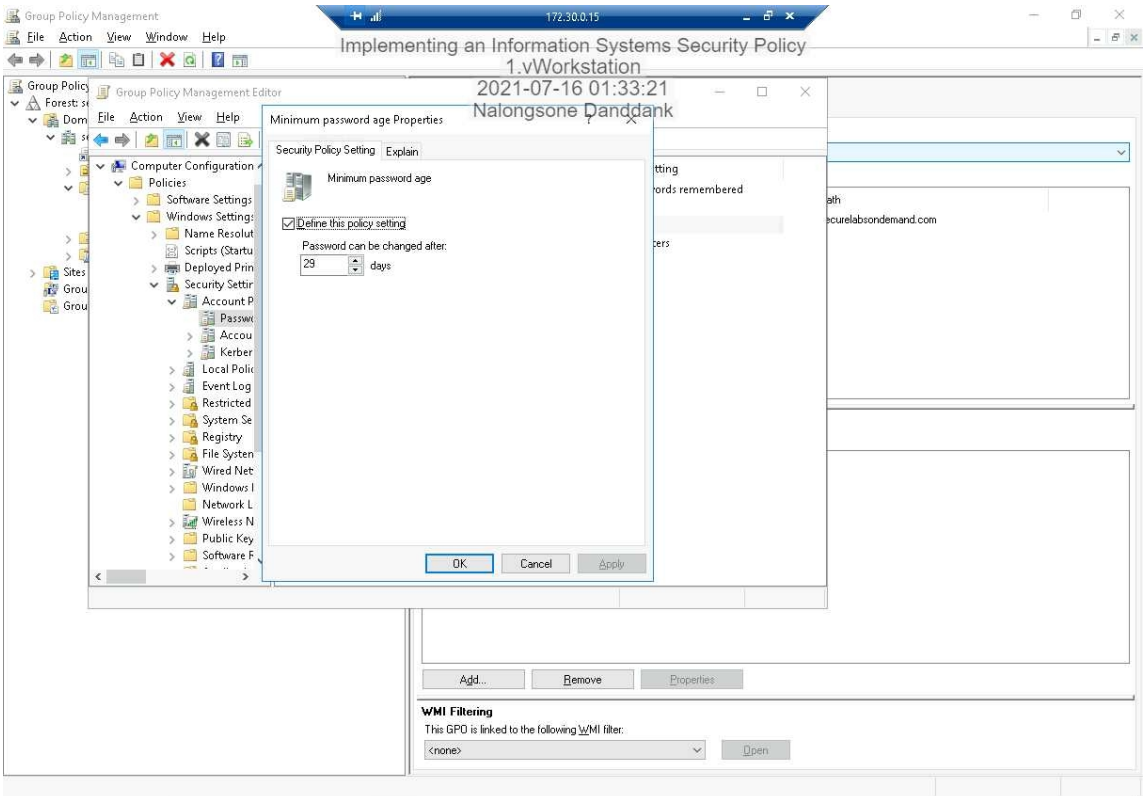

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:25:11
Nalongsone Danddank
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Scope
Links
Display links in this location:
securelabsondemand.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
securelabsondemand.com
No
Yes
securelabsondemand.com
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:25 PM
7/15/2021

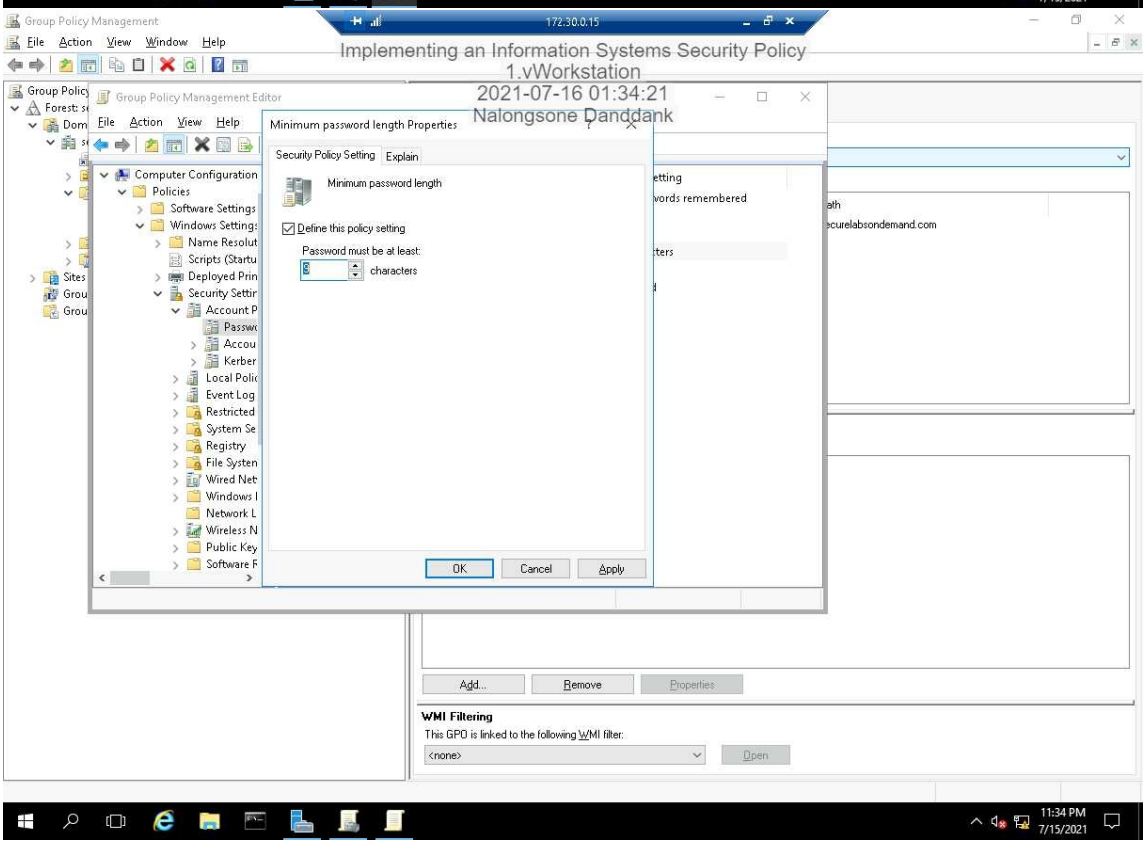

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:27:46
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
7 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:27 PM
7/15/2021

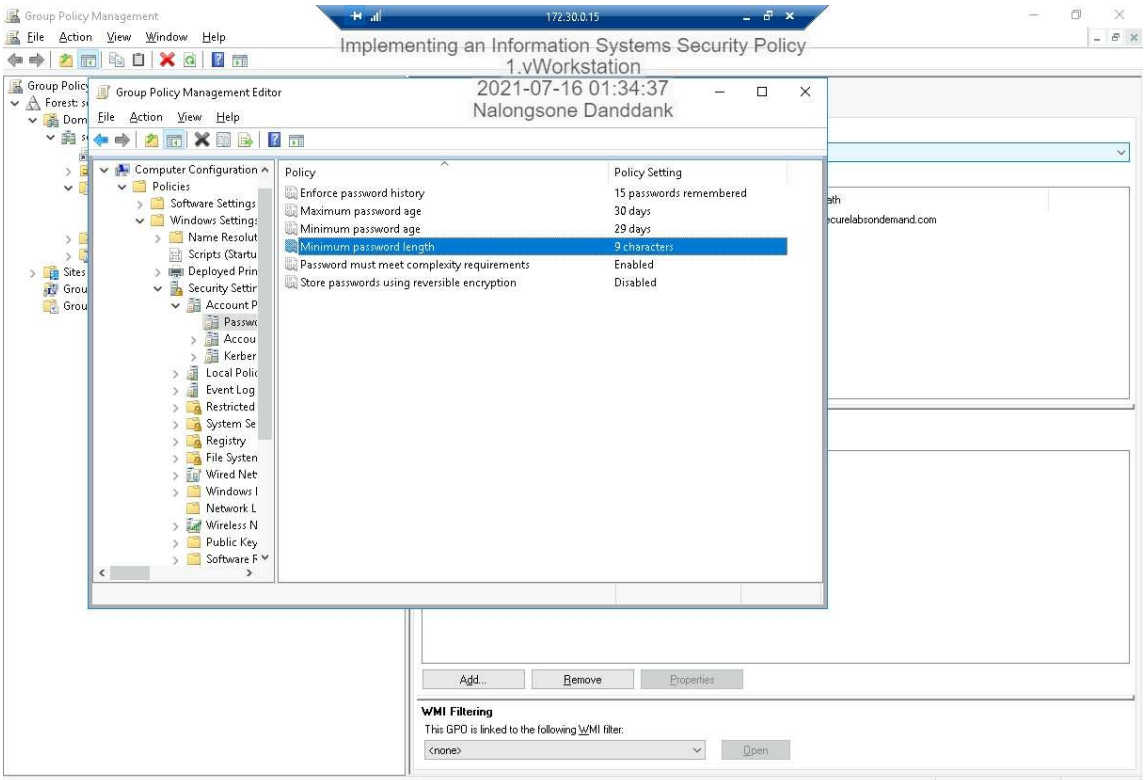

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:28:45
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
Enforce password history Properties
Security Policy Setting
Explain
Enforce password history
Define this policy setting
passwords remembered
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:28 PM
7/15/2021

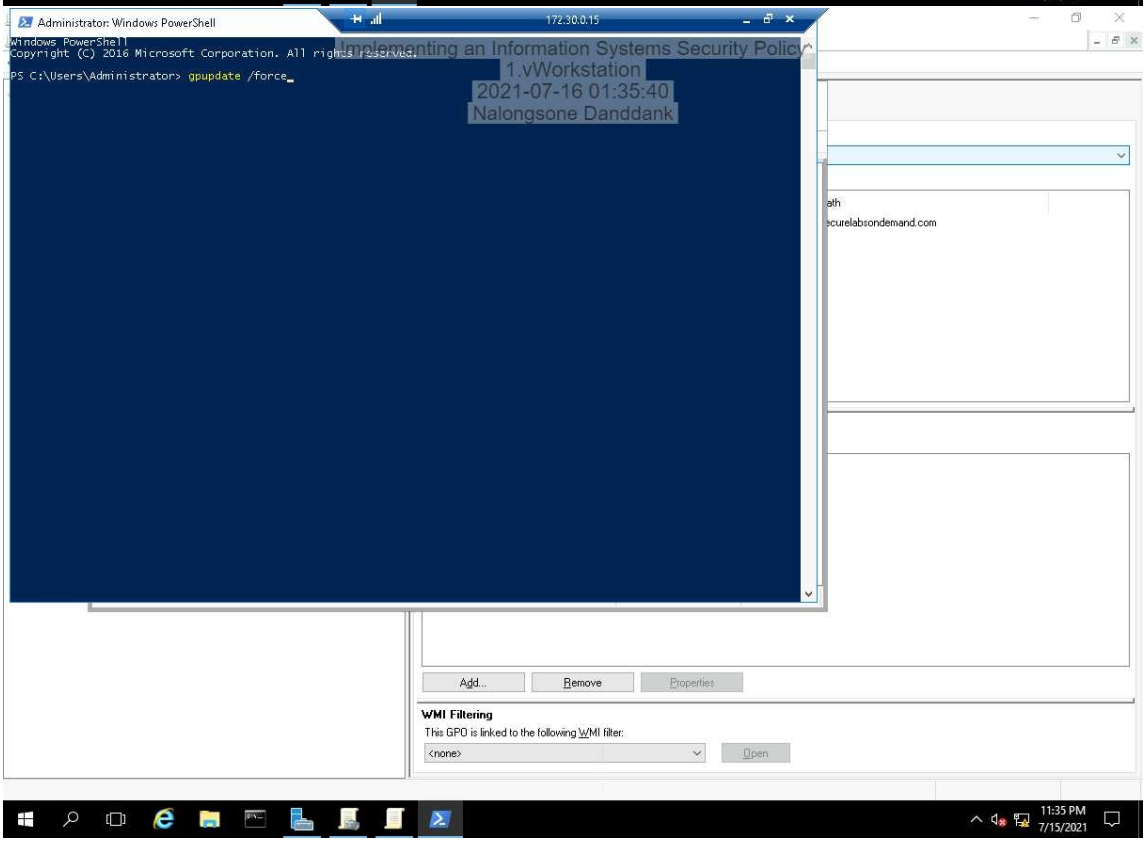

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:30:12
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
Enforce password history Properties
Security Policy Setting Explain
Enforce password history
Define this policy setting
Keep password history for:
15
passwords remembered
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:30 PM
7/15/2021

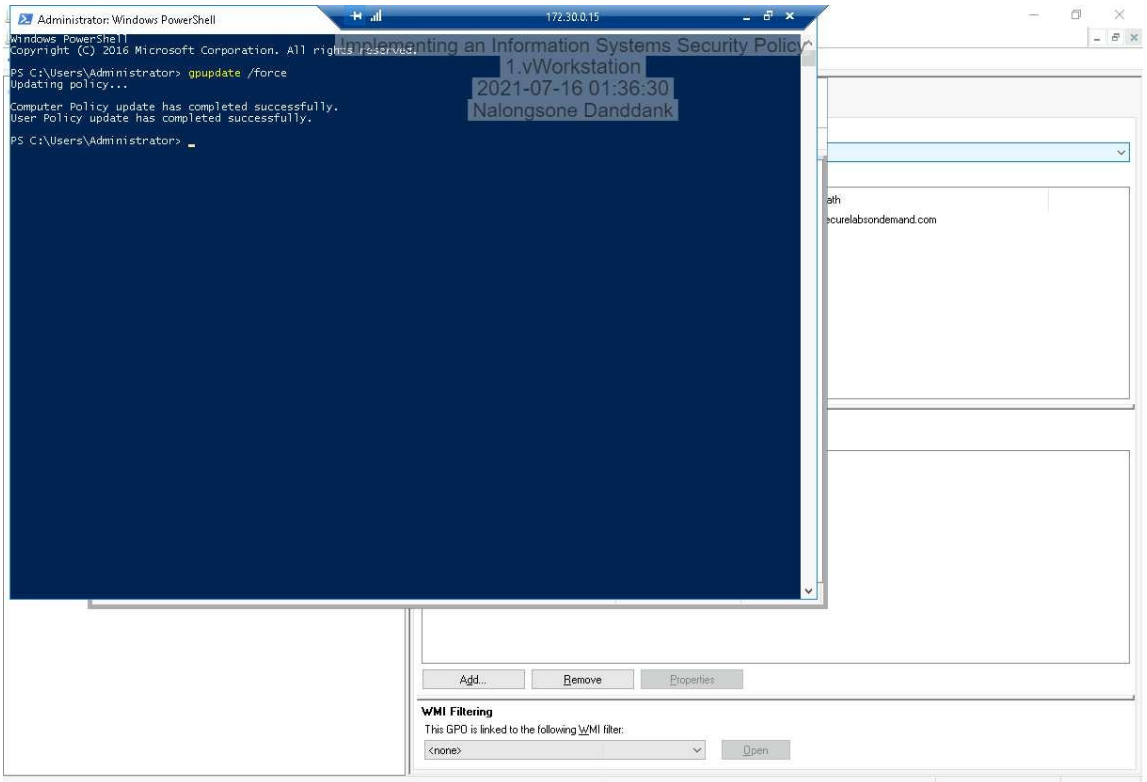

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:32:48
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
Maximum password age Properties
Security Policy Setting Explain
Maximum password age
Define this policy setting
Password will expire in:
30
days
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:32 PM
7/15/2021

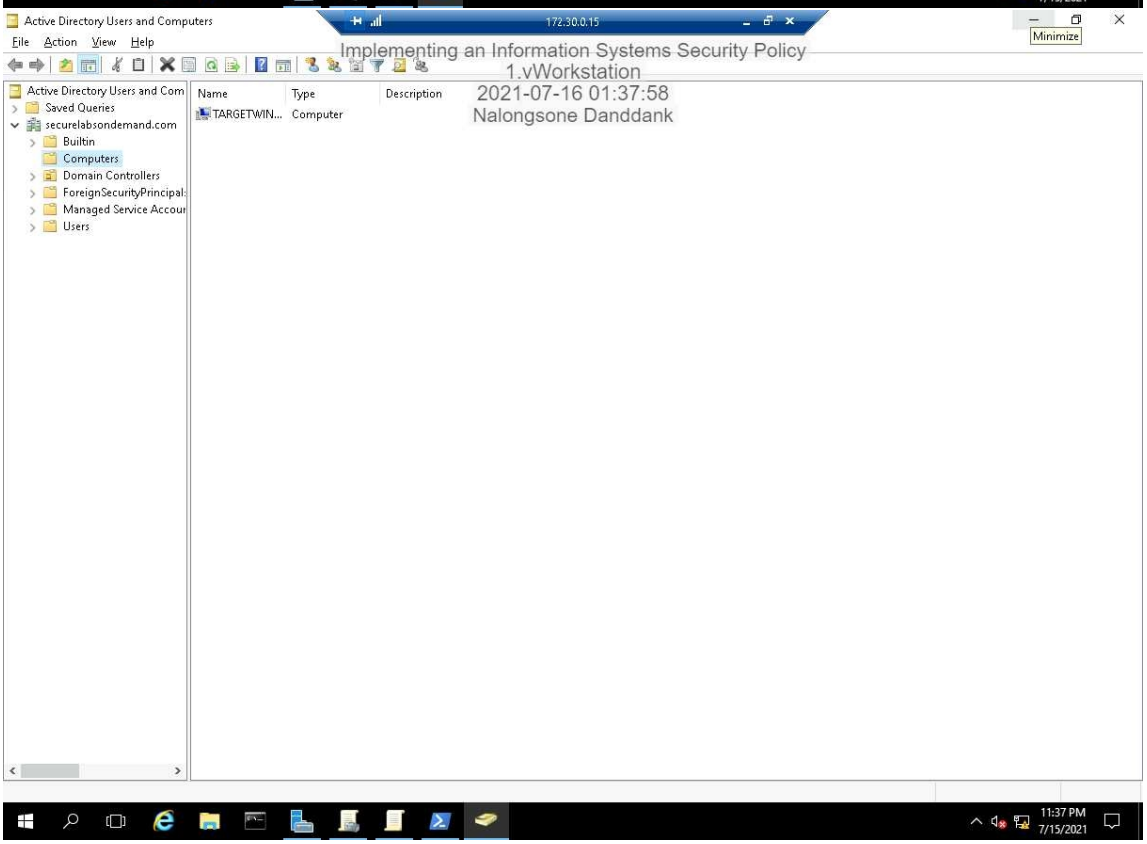

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:33:21
Nalongsone Danddank
Minimum password age Properties
Security Policy Setting
Explain
Minimum password age
Define this policy setting
Password can be changed after:
29
days
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:33 PM
7/15/2021

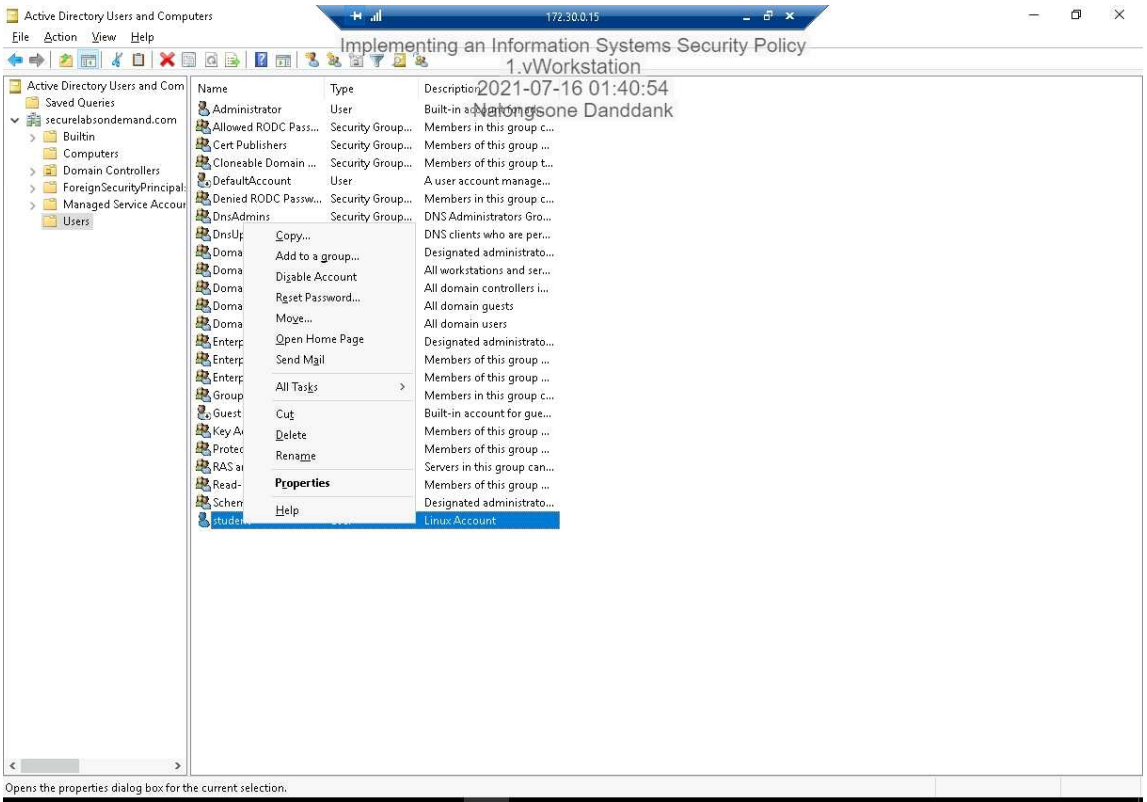

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:34:21
Nalongsone Danddank
Minimum password length Properties
Security Policy Setting
Explain
Minimum password length
Define this policy setting
Password must be at least:
8
characters
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:34 PM
7/15/2021

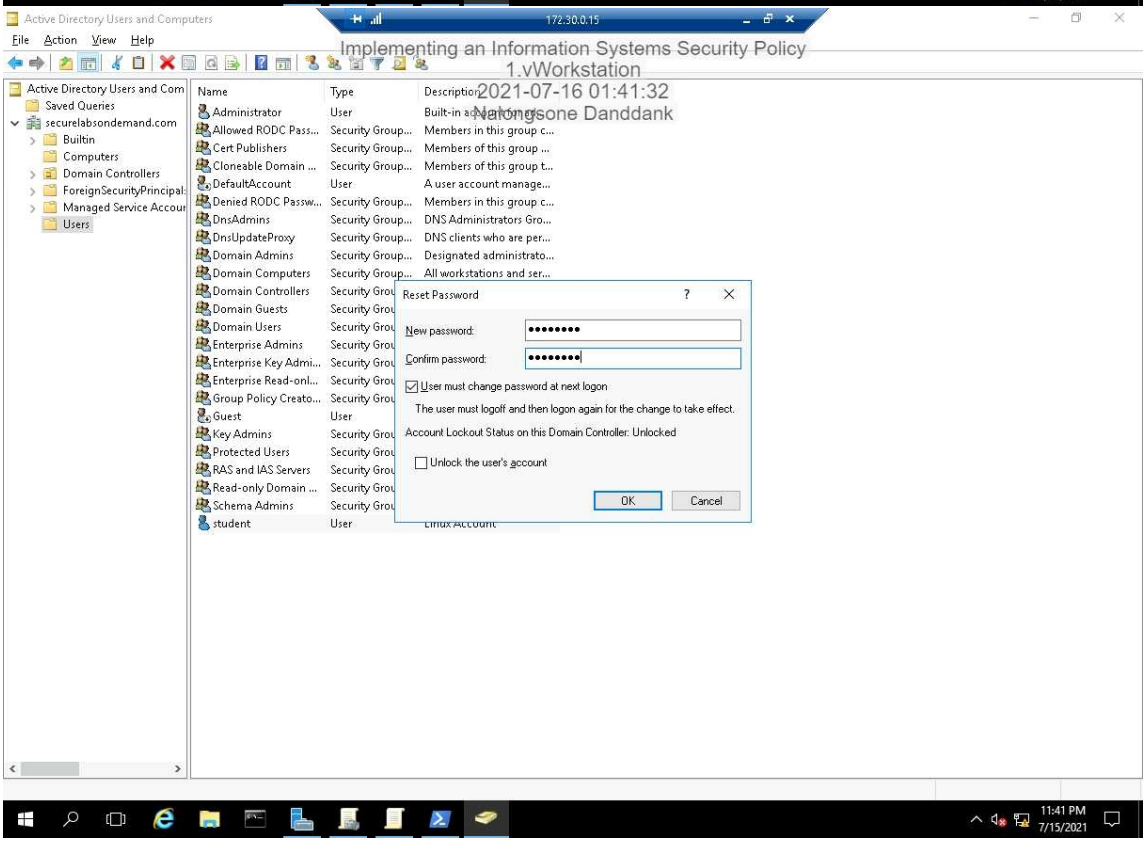

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:34:37
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Policy Setting
Enforce password history
15 passwords remembered
Maximum password age
30 days
Minimum password age
29 days
Minimum password length
9 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:34 PM
7/15/2021

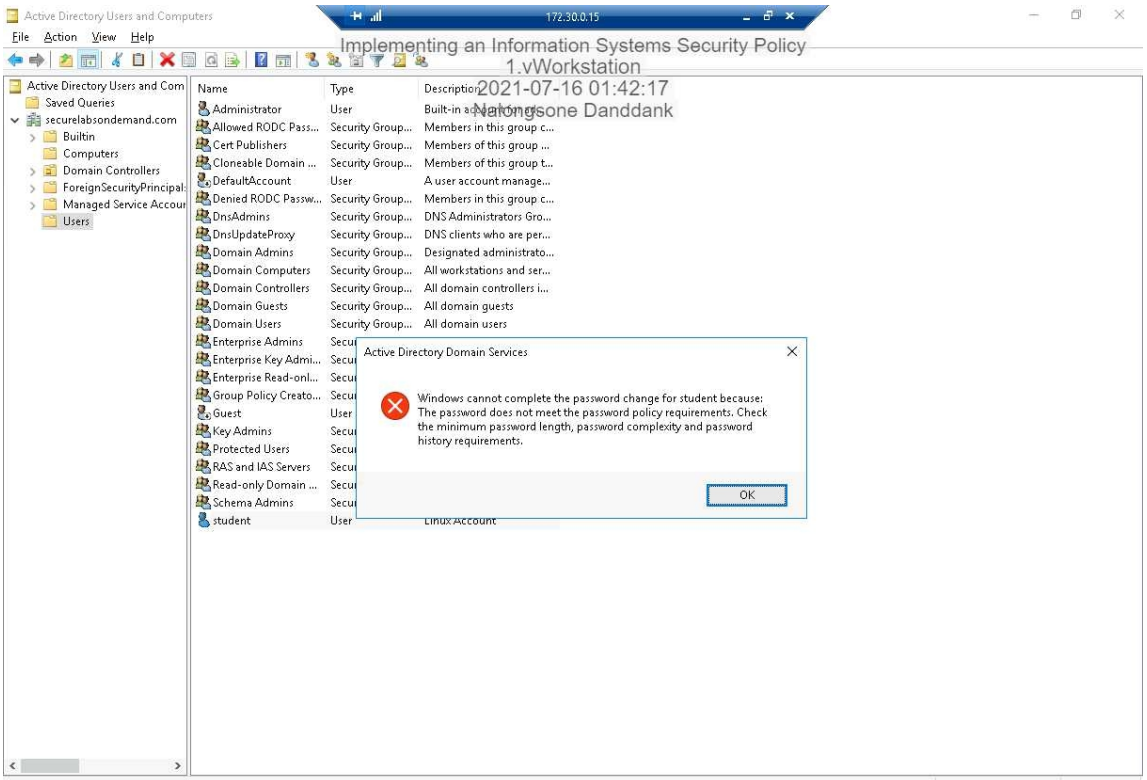

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:35:40
Nalongsone Danddank
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> gpupdate /force
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:35 PM
7/15/2021

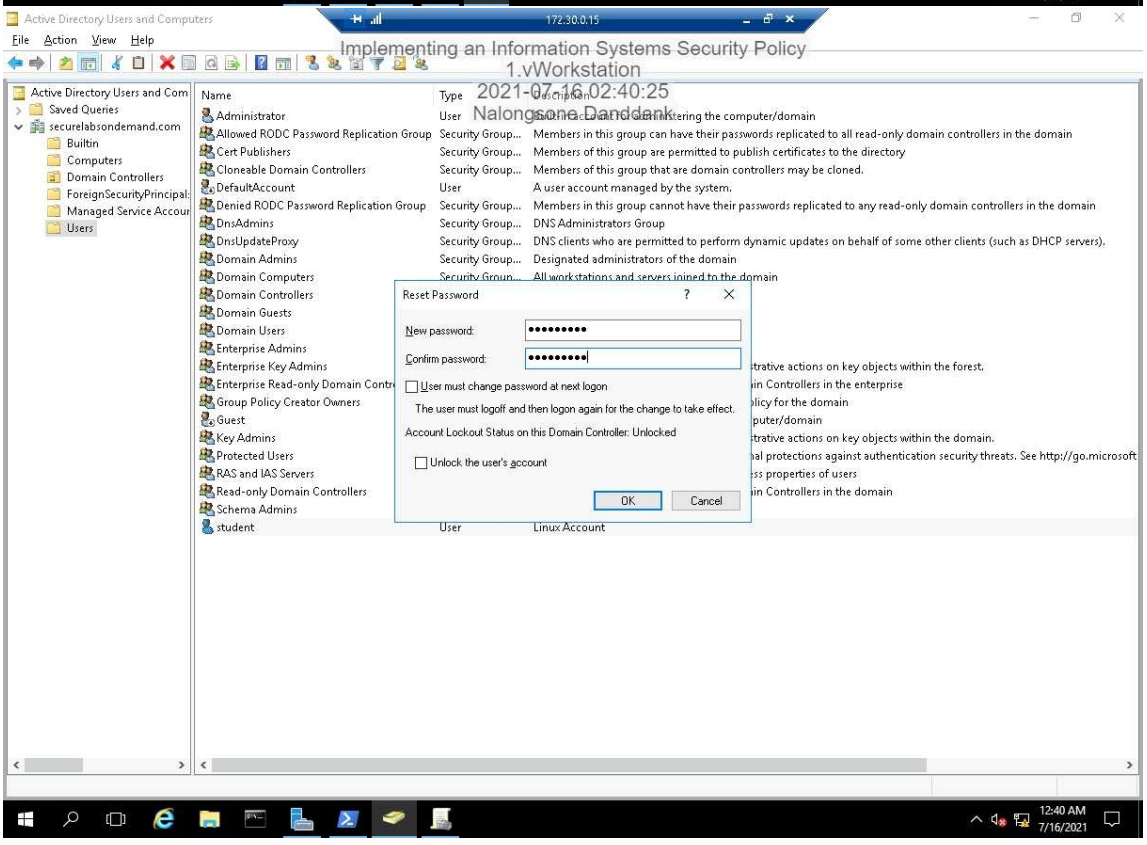

Administrator: Windows PowerShell
172.30.0.15
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\Users\Administrator>
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:36:30
Nalongsone Danddank
securelabsondemand.com
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:36 PM
7/15/2021

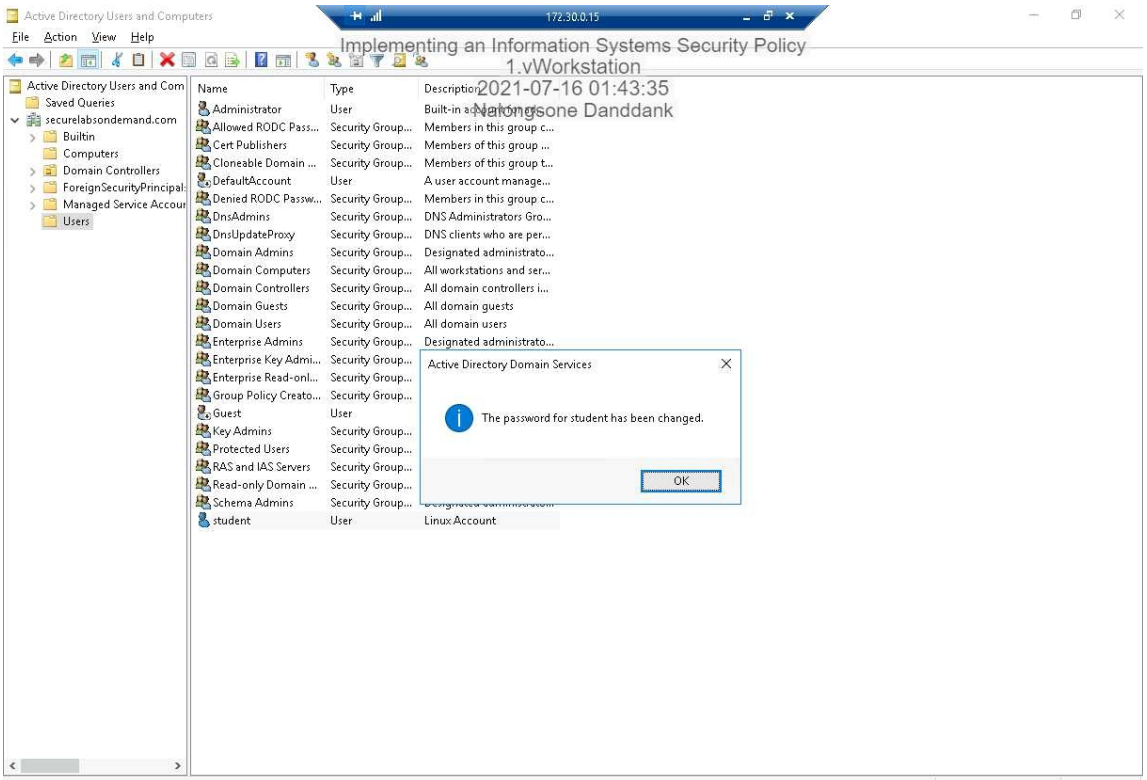

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:37:58
Nalongsone Danddank
Minimize
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
TARGETWIN...
Computer
11:37 PM
7/15/2021

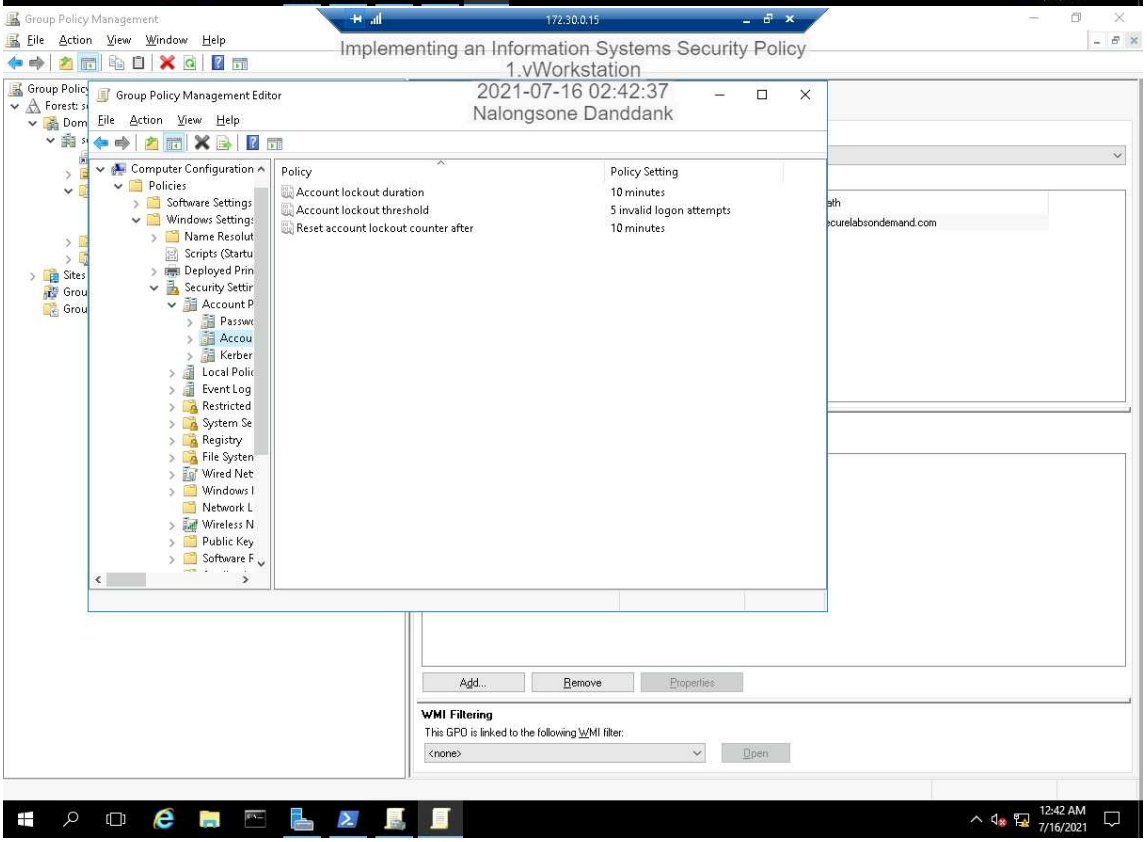

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:40:54
Nakongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
Administrator
Allowed RODC Pass...
Cert Publishers
Cloneable Domain ...
DefaultAccount
Denied RODC Passw...
DnsAdmins
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
Linux Account
Opens the properties dialog box for the current selection.
11:40 PM
7/15/2021

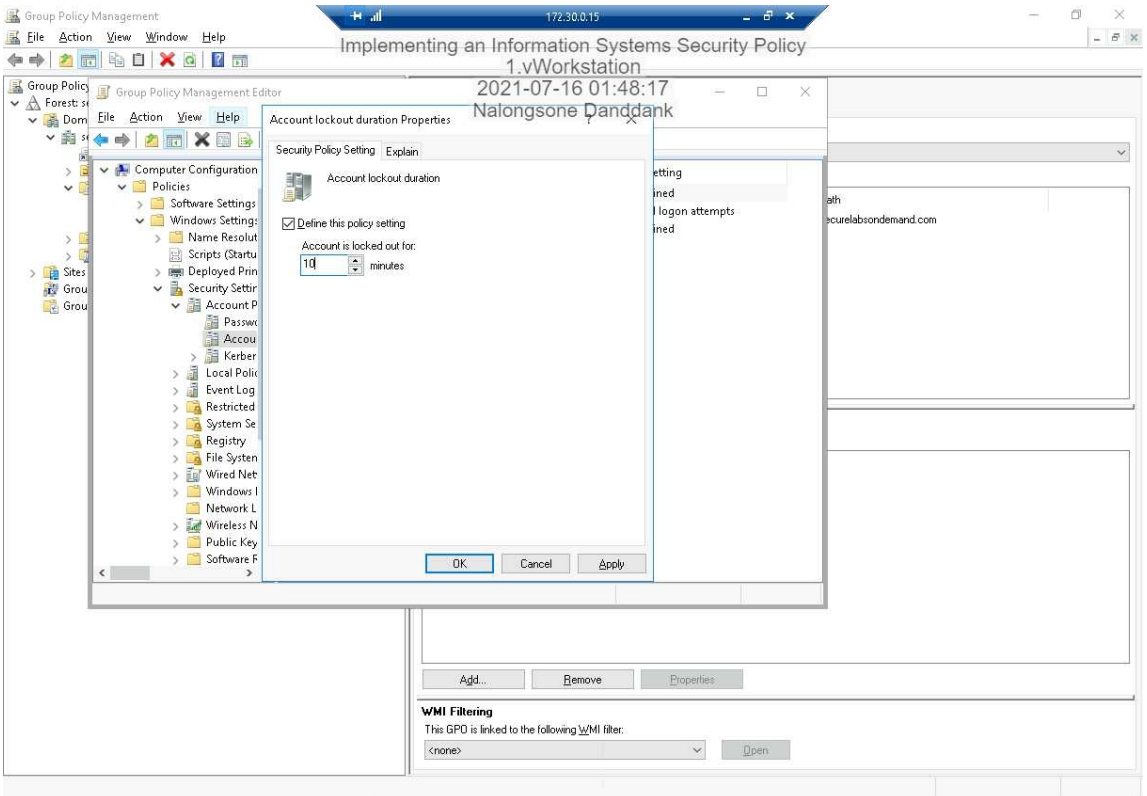

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:41:32
Nakongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
Reset Password
New password:
Confirm password:
User must change password at next logon
The user must logoff and then logon again for the change to take effect.
Account Lockout Status on this Domain Controller: Unlocked
Unlock the user's account
OK
Cancel
11:41 PM
7/15/2021

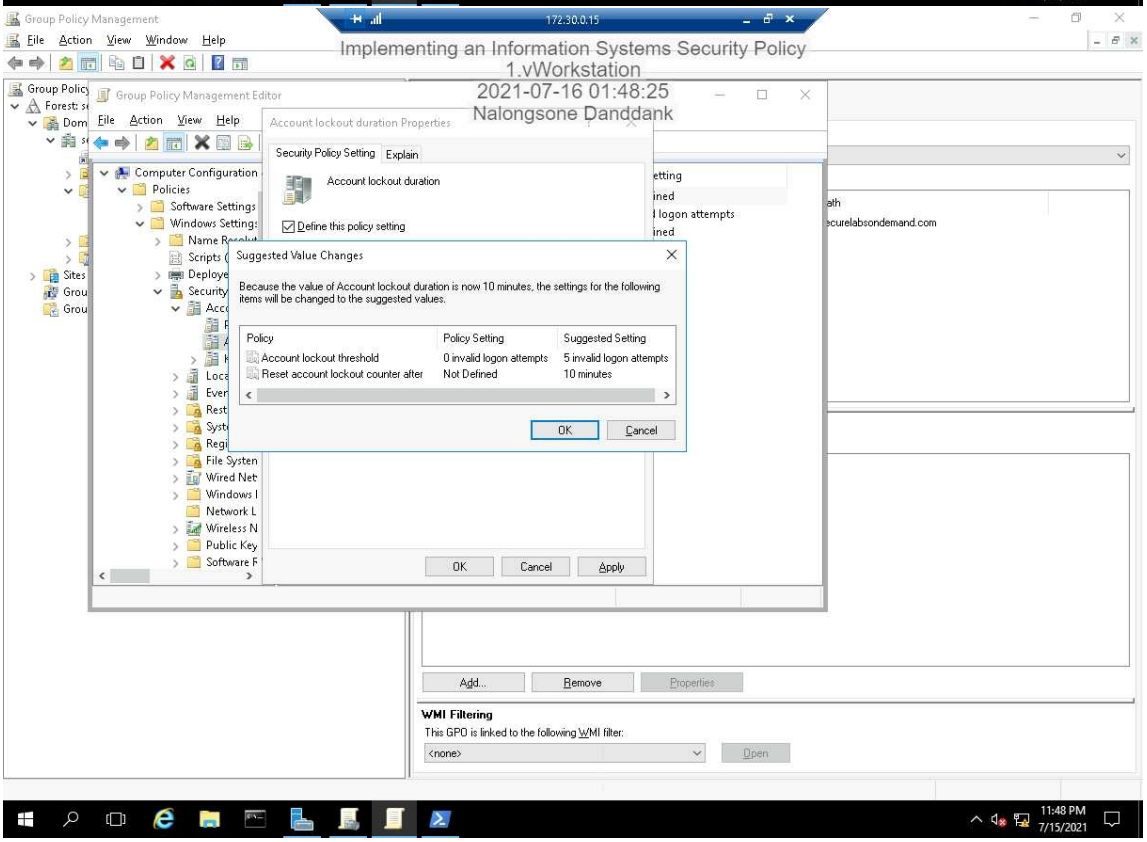

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:42:17
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
Administrator
User
Allowed RODC Pass...
Security Group...
Members in this group c...
Cert Publishers
Security Group...
Members of this group ...
Cloneable Domain ...
Security Group...
Members of this group t...
DefaultAccount
User
A user account manage...
Denied RODC Passw...
Security Group...
Members in this group c...
DnsAdmins
Security Group...
DNS Administrators Gro...
DnsUpdateProxy
Security Group...
DNS clients who are per...
Domain Admins
Security Group...
Designated administrato...
Domain Computers
Security Group...
All workstations and ser...
Domain Controllers
Security Group...
All domain controllers i...
Domain Guests
Security Group...
All domain guests
Domain Users
Security Group...
All domain users
Enterprise Admins
Enterprise Key Admi...
Enterprise Read-onl...
Group Policy Creato...
Guest
User
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain ...
Schema Admins
student
User
Linux Account
Active Directory Domain Services
Windows cannot complete the password change for student because:
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
OK
11:42 PM
7/15/2021

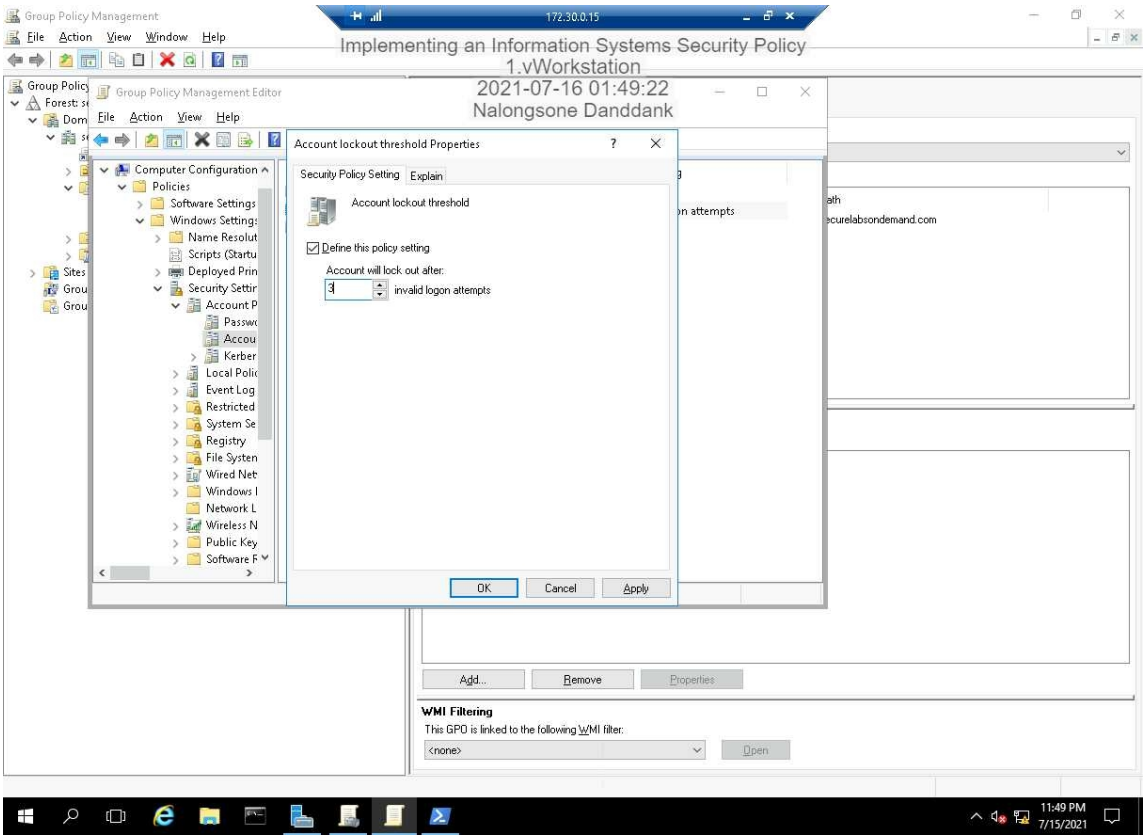

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 02:40:25
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
Administrator
User
Built-in account for administering the computer/domain
Allowed RODC Password Replication Group
Security Group...
Members in this group can have their passwords replicated to all read-only domain controllers in the domain
Cert Publishers
Security Group...
Members of this group are permitted to publish certificates to the directory
Cloneable Domain Controllers
Security Group...
Members of this group that are domain controllers may be cloned.
DefaultAccount
User
A user account managed by the system.
Denied RODC Password Replication Group
Security Group...
Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain
DnsAdmins
Security Group...
DNS Administrators Group
DnsUpdateProxy
Security Group...
DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Domain Admins
Security Group...
Designated administrators of the domain
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Key Admins
Enterprise Read-only Domain Contr
Group Policy Creator Owners
Guest
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
student
User
Linux Account
Reset Password
New password:
Confirm password:
User must change password at next logon
The user must logoff and then logon again for the change to take effect.
Account Lockout Status on this Domain Controller: Unlocked
Unlock the user's account
OK
Cancel
12:40 AM
7/16/2021

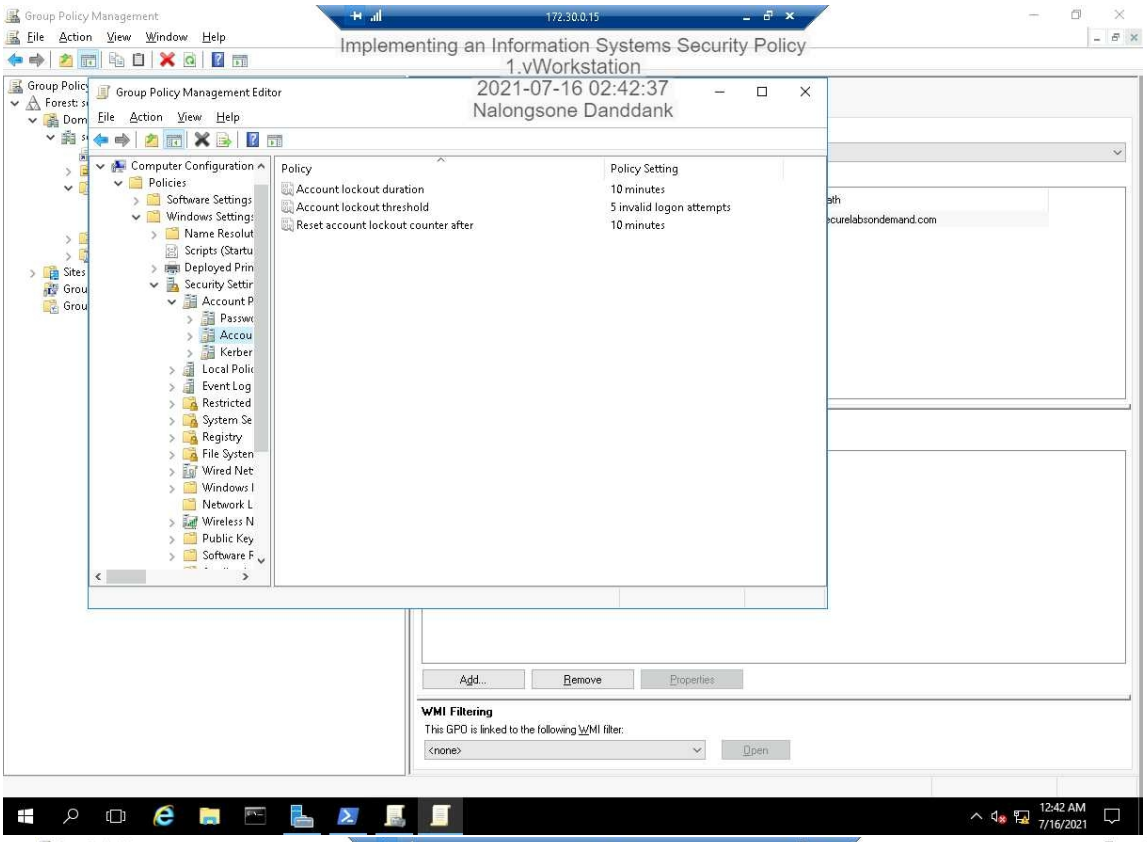

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:43:35
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
Administrator
User
Built-in account for...
Allowed RODC Pass...
Security Group...
Members in this group c...
Cert Publishers
Security Group...
Members of this group ...
Cloneable Domain ...
Security Group...
Members of this group t...
DefaultAccount
User
A user account manage...
Denied RODC Passw...
Security Group...
Members in this group c...
DnsAdmins
Security Group...
DNS Administrators Gro...
DnsUpdateProxy
Security Group...
DNS clients who are per...
Domain Admins
Security Group...
Designated administrato...
Domain Computers
Security Group...
All workstations and ser...
Domain Controllers
Security Group...
All domain controllers i...
Domain Guests
Security Group...
All domain guests
Domain Users
Security Group...
All domain users
Enterprise Admins
Security Group...
Designated administrato...
Enterprise Key Admi...
Security Group...
Enterprise Read-onl...
Security Group...
Group Policy Creato...
Security Group...
Guest
User
Key Admins
Security Group...
Protected Users
Security Group...
RAS and IAS Servers
Security Group...
Read-only Domain ...
Security Group...
Schema Admins
Security Group...
student
User
Linux Account
Active Directory Domain Services
The password for student has been changed.
OK
11:43 PM
7/15/2021

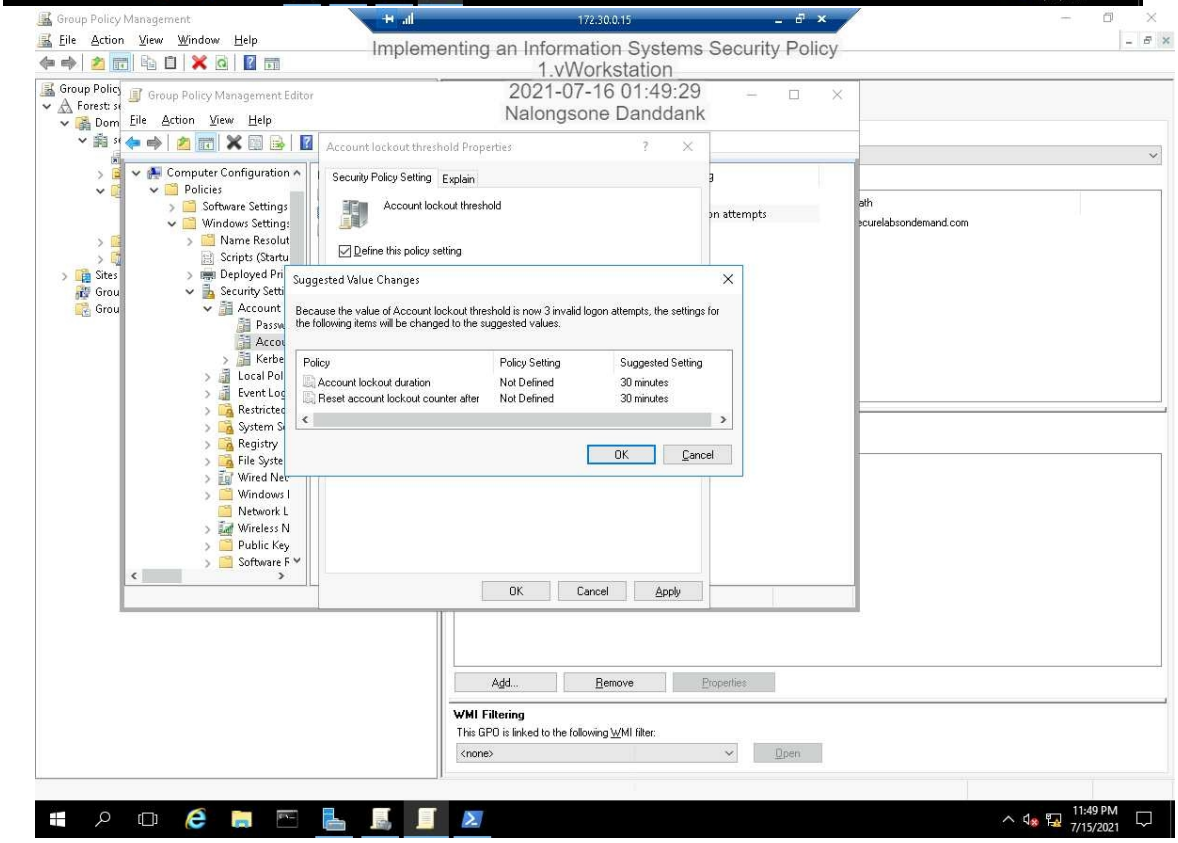

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 02:42:37
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Setting:
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
10 minutes
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
12:42 AM
7/16/2021

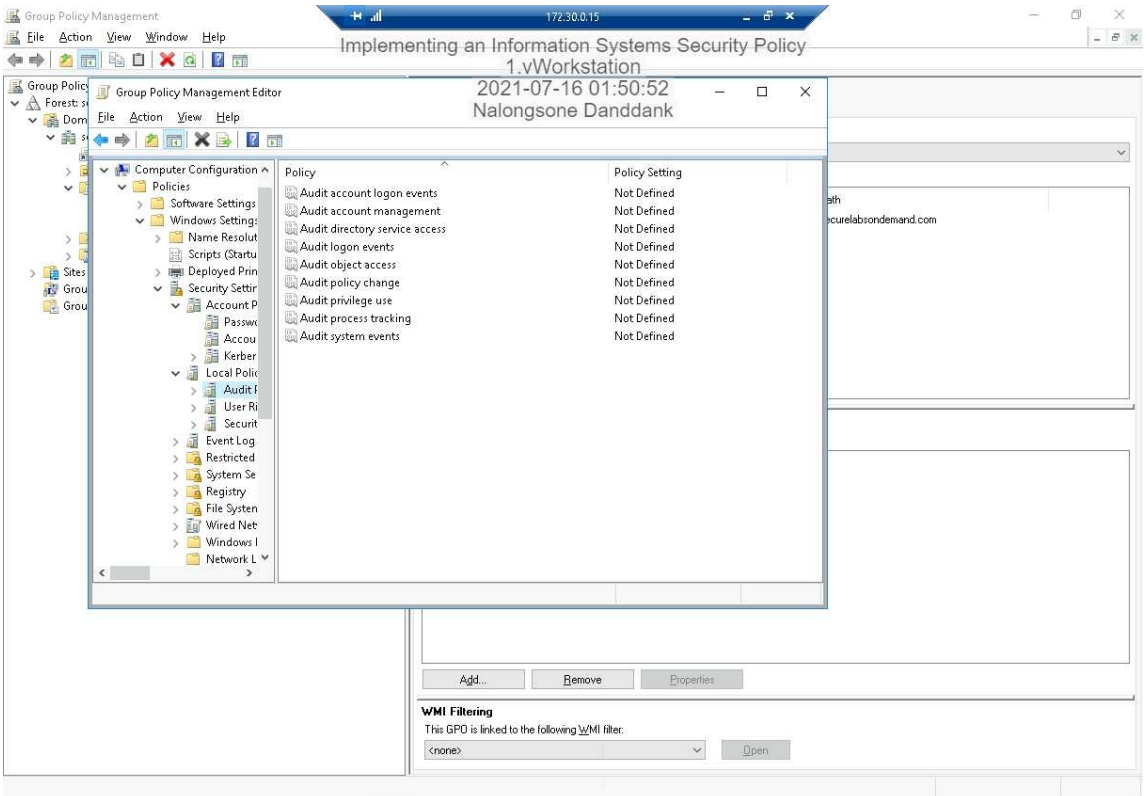

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:48:17
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Account lockout duration Properties
Security Policy Setting Explain
Account lockout duration
Define this policy setting
Account is locked out for:
10
minutes
OK Cancel Apply
Computer Configuration
Policies
Software Settings
Windows Settings
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:48 PM
7/15/2021

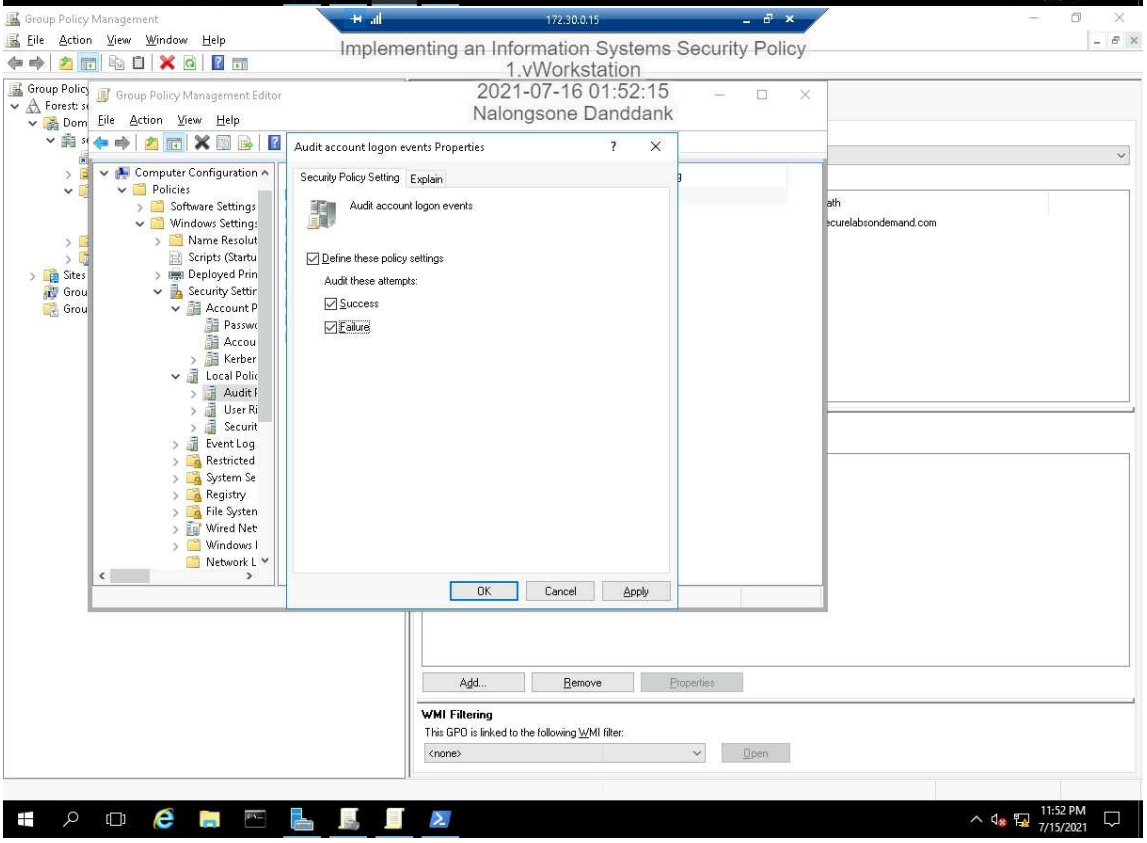

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:48:25
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
Account lockout duration Properties
Security Policy Setting Explain
Account lockout duration
Define this policy setting
Suggested Value Changes
Because the value of Account lockout duration is now 10 minutes, the settings for the following items will be changed to the suggested values.
Policy
Policy Setting
Suggested Setting
Account lockout threshold
0 invalid logon attempts
5 invalid logon attempts
Reset account lockout counter after
Not Defined
10 minutes
OK Cancel
OK Cancel Apply
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:48 PM
7/15/2021

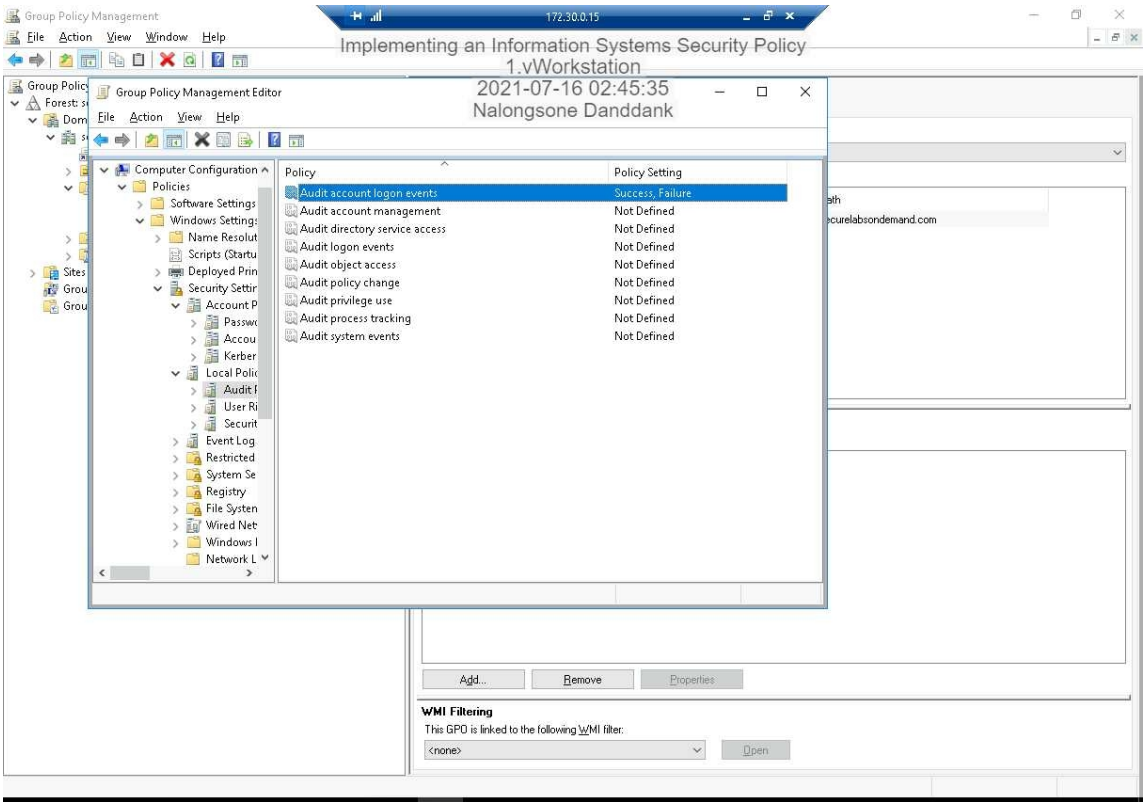

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:49:22
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Account lockout threshold Properties
Security Policy Setting
Explain
Account lockout threshold
Define this policy setting
Account will lock out after:
3
invalid logon attempts
OK
Cancel
Apply
Computer Configuration
Policies
Software Settings
Windows Setting:
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:49 PM
7/15/2021

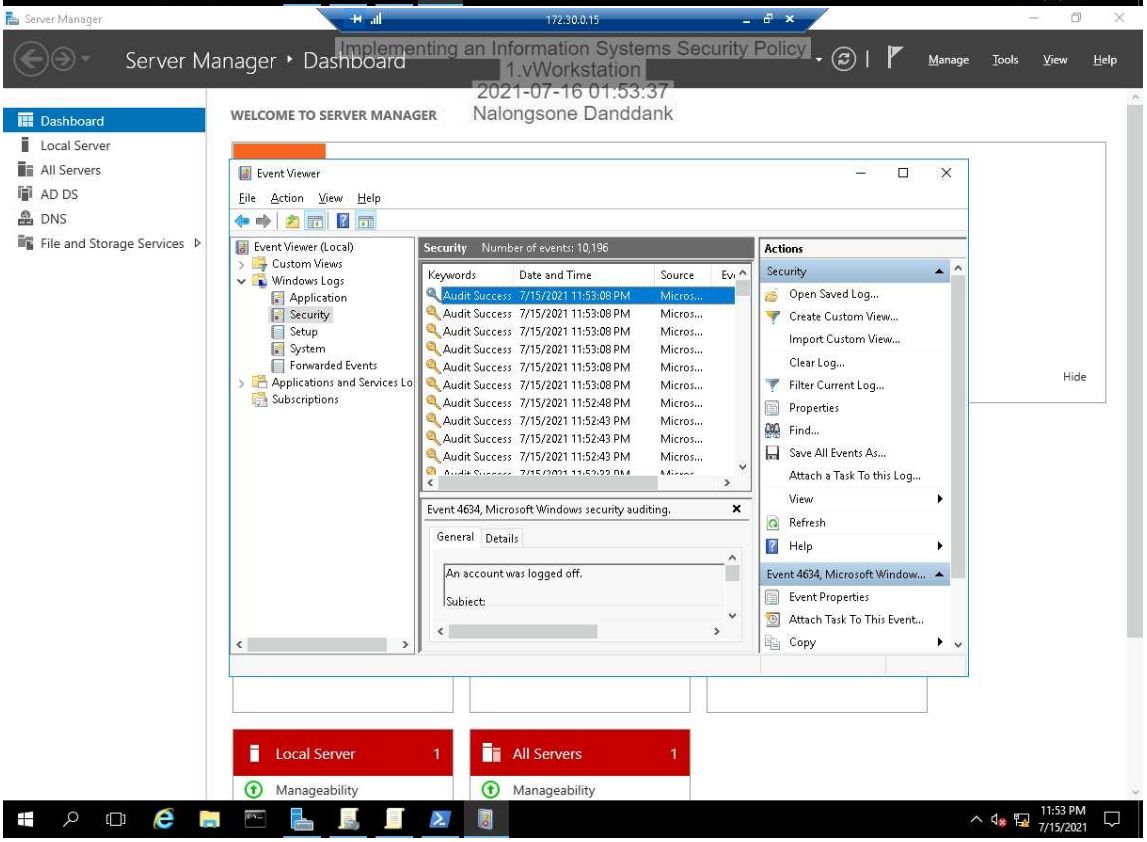

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 02:42:37
Nalongsone Danddank
Group Policy Management Editor
Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
10 minutes
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
12:42 AM
7/16/2021

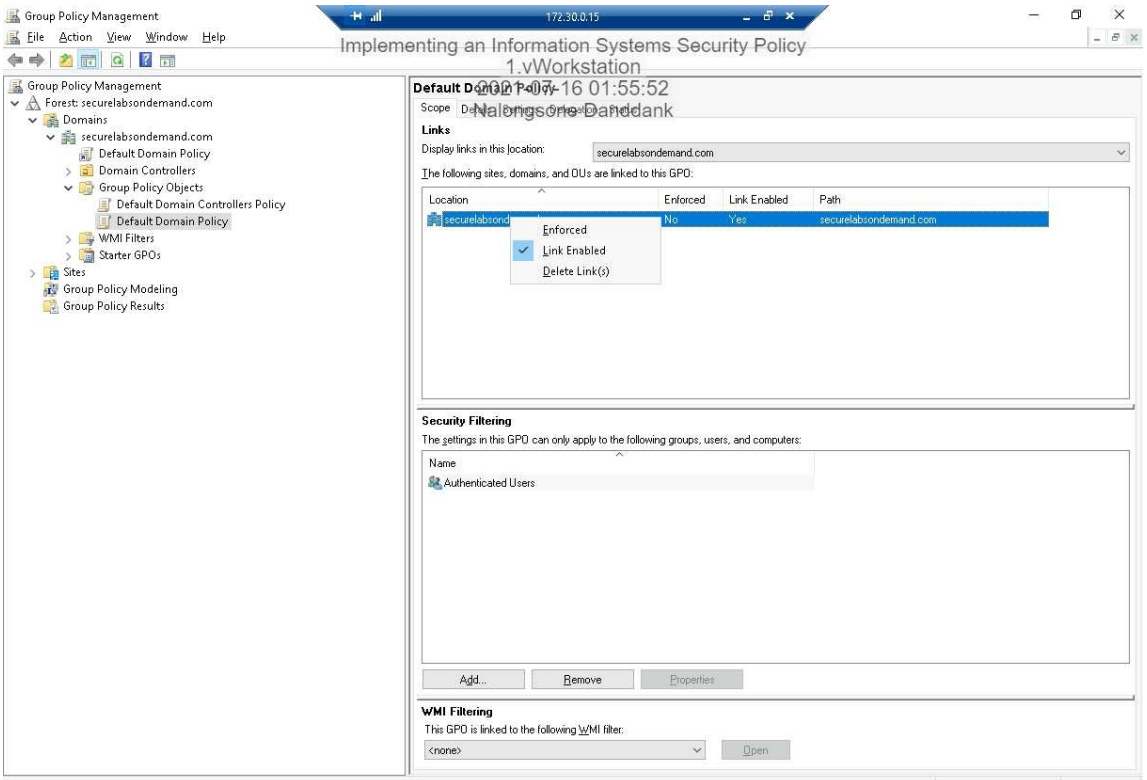

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:49:29
Nalongsone Danddank
Group Policy Management Editor
Account lockout threshold Properties
Security Policy Setting
Explain
Account lockout threshold
Define this policy setting
Suggested Value Changes
Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.
Policy
Policy Setting
Suggested Setting
Account lockout duration
Not Defined
30 minutes
Reset account lockout counter after
Not Defined
30 minutes
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:49 PM
7/15/2021

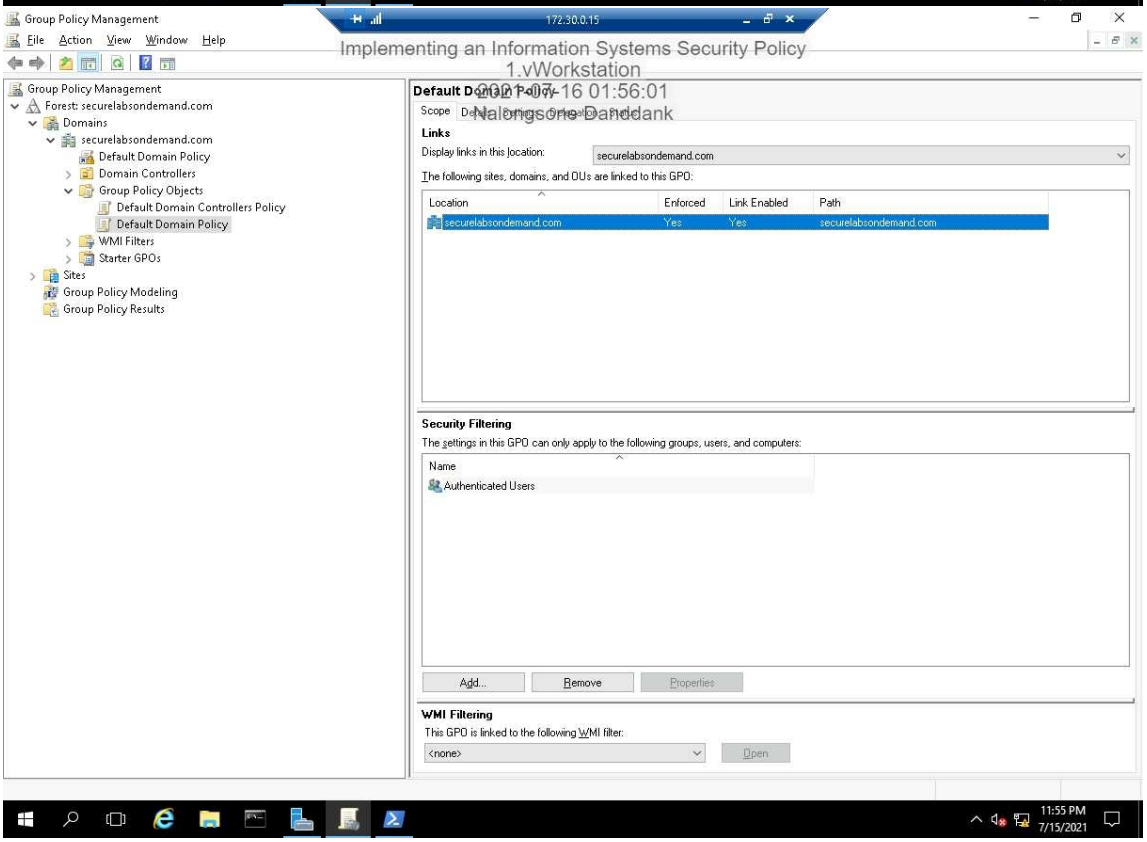

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:50:52
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Policy
Policy Setting
Audit account logon events Not Defined
Audit account management Not Defined
Audit directory service access Not Defined
Audit logon events Not Defined
Audit object access Not Defined
Audit policy change Not Defined
Audit privilege use Not Defined
Audit process tracking Not Defined
Audit system events Not Defined
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:50 PM
7/15/2021

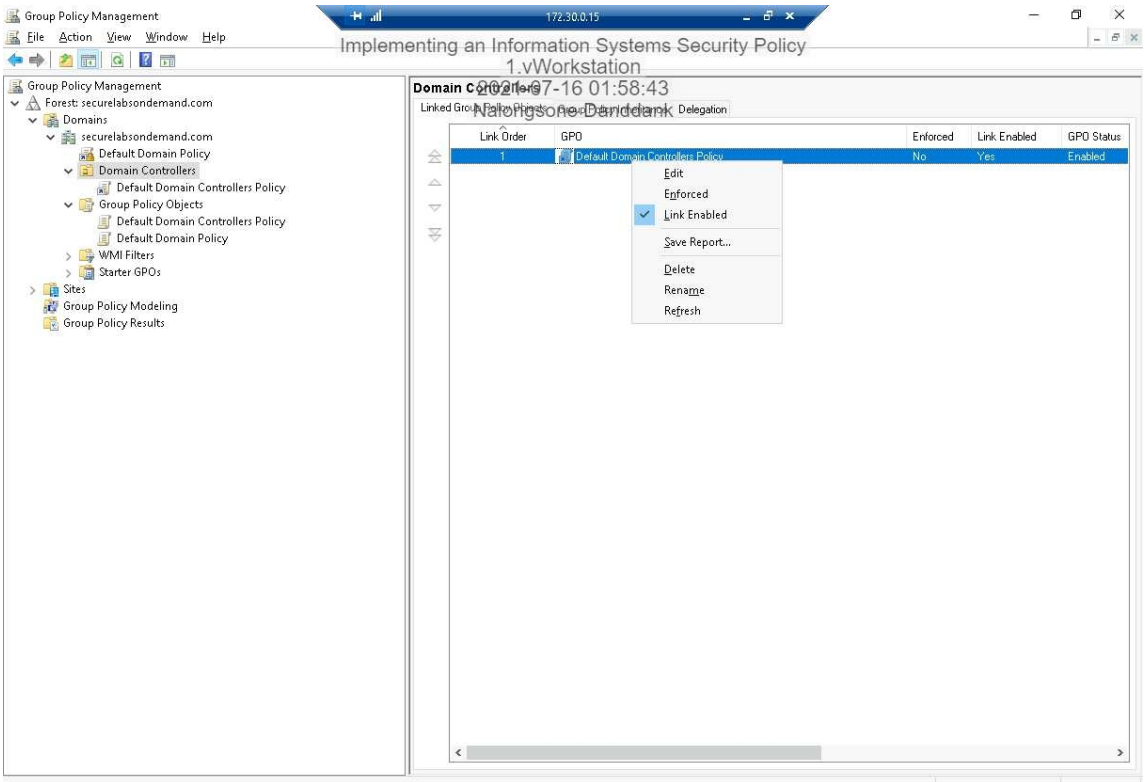

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:52:15
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Audit account logon events Properties
Security Policy Setting
Explain
Audit account logon events
Define these policy settings
Audit these attempts:
Success
Failure
OK
Cancel
Apply
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:52 PM
7/15/2021

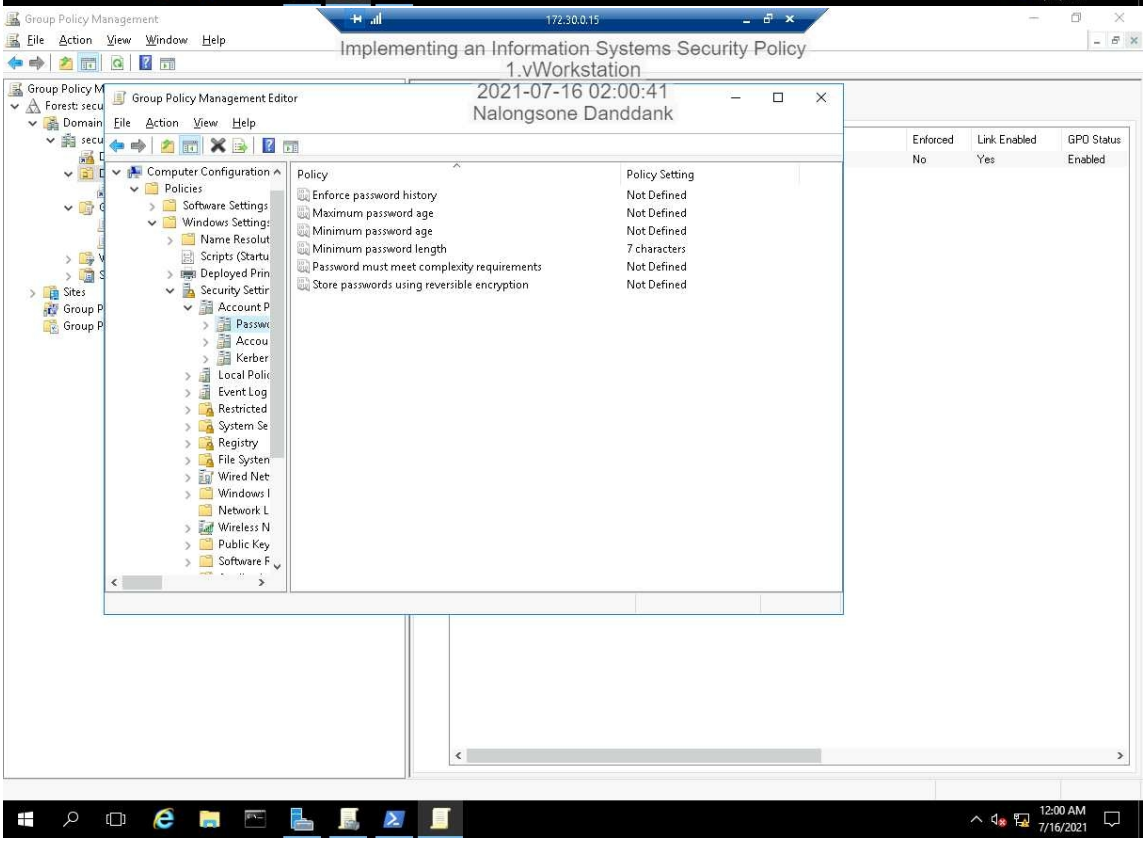

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 02:45:35
Nalongsone Danddank
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Policy
Policy Setting
Audit account logon events
Success, Failure
Audit account management
Not Defined
Audit directory service access
Not Defined
Audit logon events
Not Defined
Audit object access
Not Defined
Audit policy change
Not Defined
Audit privilege use
Not Defined
Audit process tracking
Not Defined
Audit system events
Not Defined
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
12:45 AM
7/16/2021

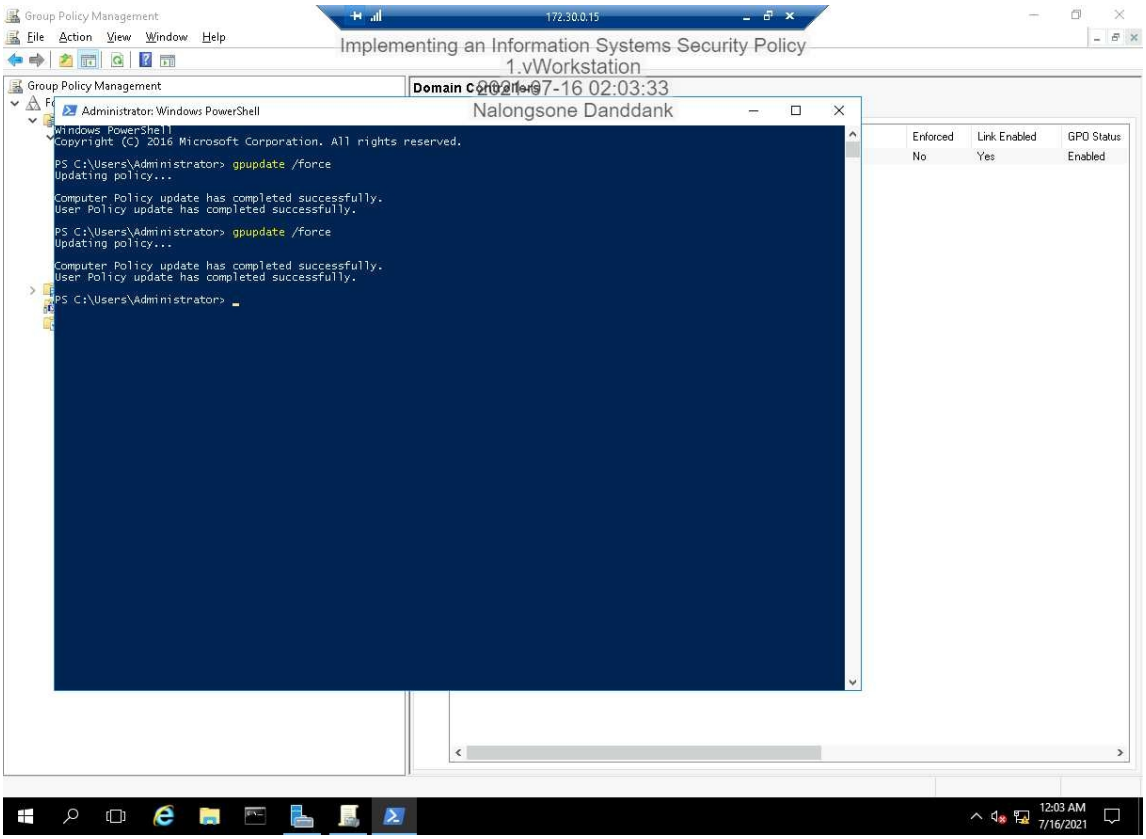

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:53:37
Nalongsone Danddank
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 10,196
Keywords Date and Time Source
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:53:08 PM Micros...
Audit Success 7/15/2021 11:52:48 PM Micros...
Audit Success 7/15/2021 11:52:43 PM Micros...
Audit Success 7/15/2021 11:52:43 PM Micros...
Audit Success 7/15/2021 11:52:43 PM Micros...
Event 4634, Microsoft Windows security auditing.
General Details
An account was logged off.
Subject:
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4634, Microsoft Window...
Event Properties
Attach Task To This Event...
Copy
Hide
Local Server 1
Manageability
All Servers 1
Manageability
11:53 PM
7/15/2021


Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:55:52
Nalongsone Danddank
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope
Links
Display links in this location:
securelabsondemand.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
securelabsond
No
Yes
securelabsondemand.com
Enforced
Link Enabled
Delete Link(s)
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:55 PM
7/15/2021

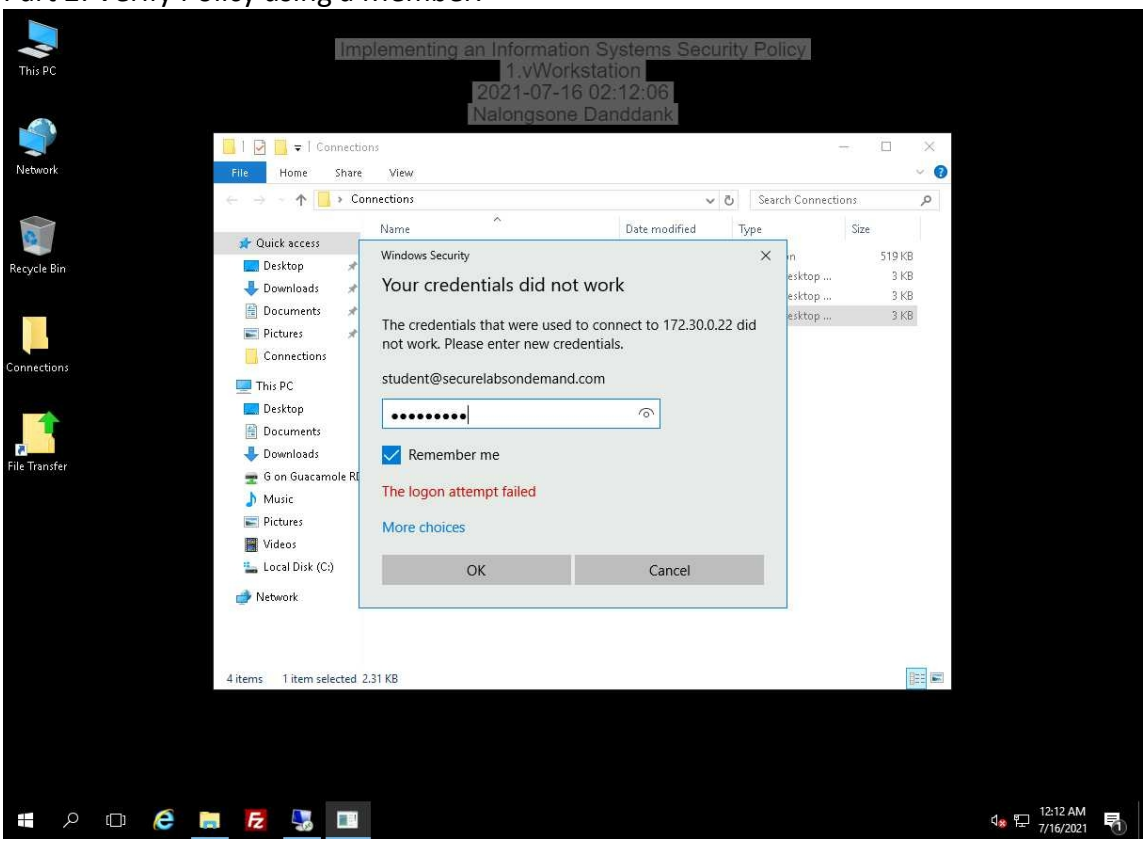

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:56:01
Nalongsone Danddank
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope
Links
Display links in this location:
securelabsondemand.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
securelabsondemand.com
Yes
Yes
securelabsondemand.com
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
11:55 PM
7/15/2021

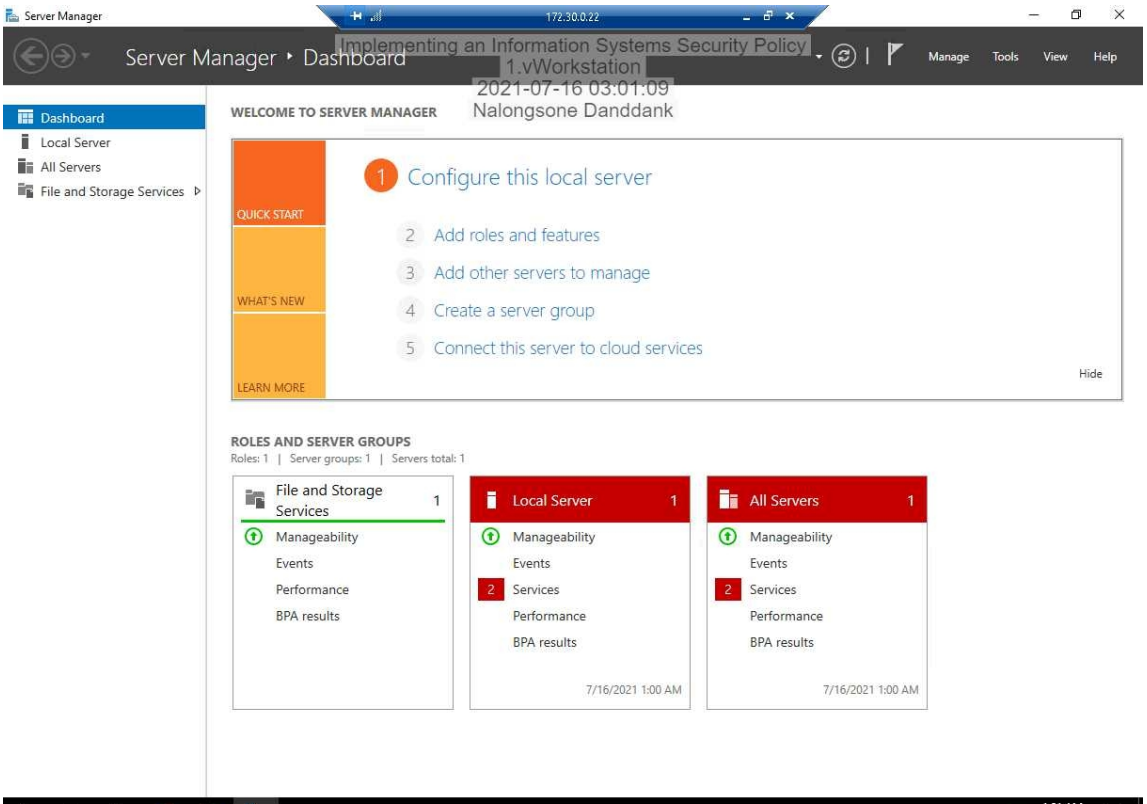

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 01:58:43
Nalongsone Danddank
Group Policy Management
Forest: securelabsondemand.com
Domains
securelabsondemand.com
Default Domain Policy
Domain Controllers
Default Domain Controllers Policy
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Domain Controllers
Linked Group Policy Objects
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
Default Domain Controllers Policy
No
Yes
Enabled
Edit
Enforced
Link Enabled
Save Report...
Delete
Rename
Refresh
11:58 PM
7/15/2021

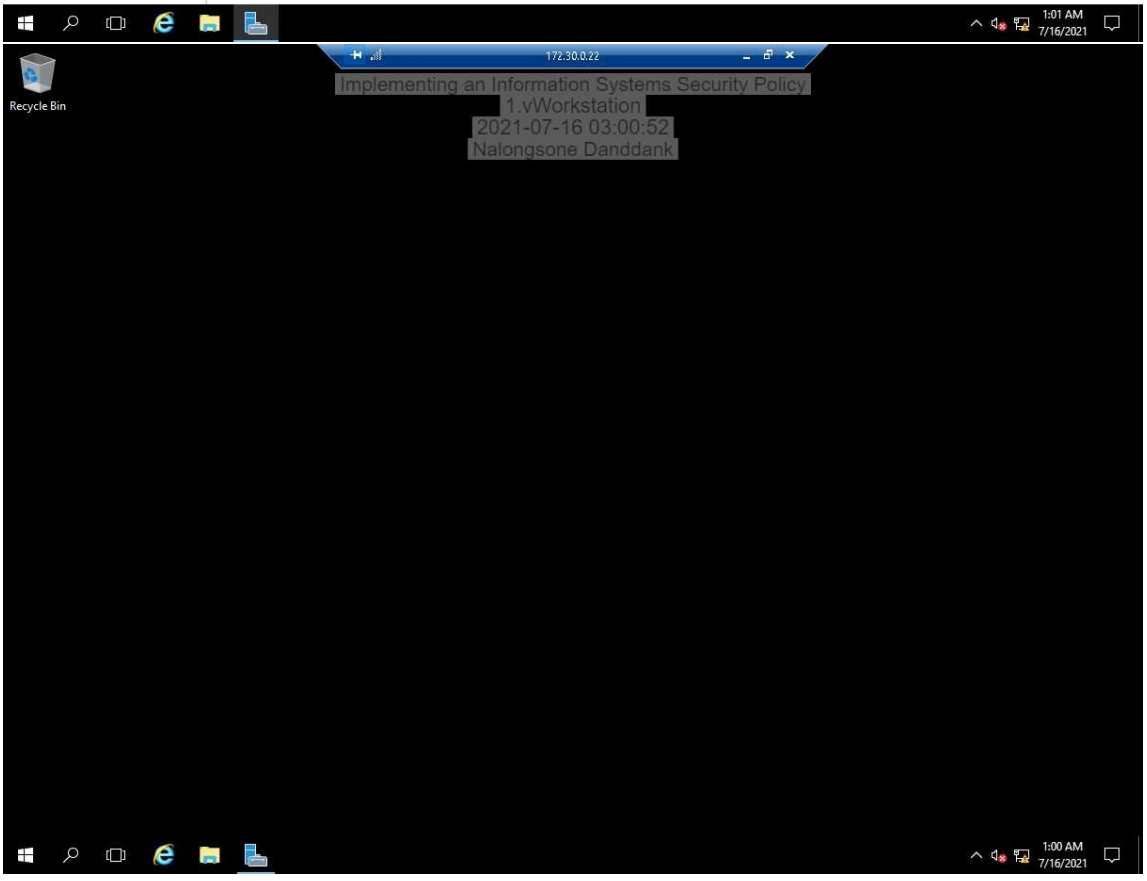

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 02:00:41
Nalongsone Danddank
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
7 characters
Password must meet complexity requirements
Not Defined
Store passwords using reversible encryption
Not Defined
Enforced
Link Enabled
GPO Status
No
Yes
Enabled
12:00 AM
7/16/2021

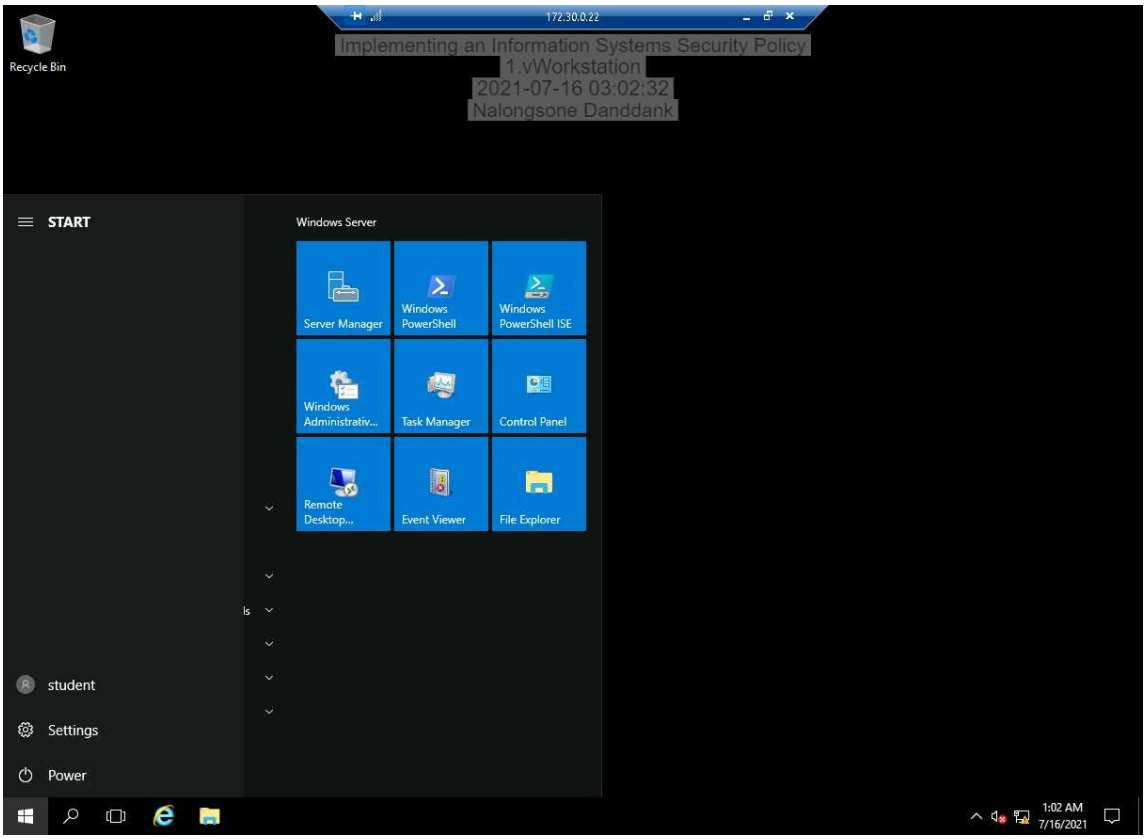


Part 2: Verify Policy using a Member.

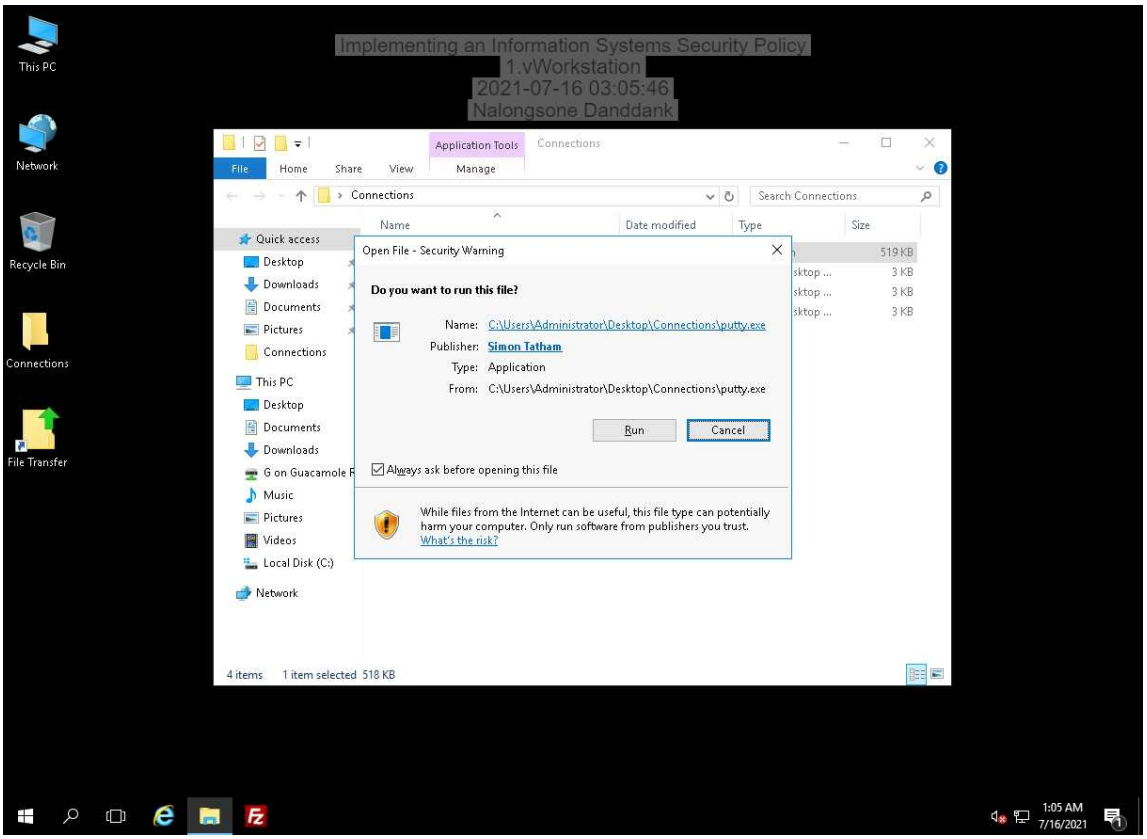


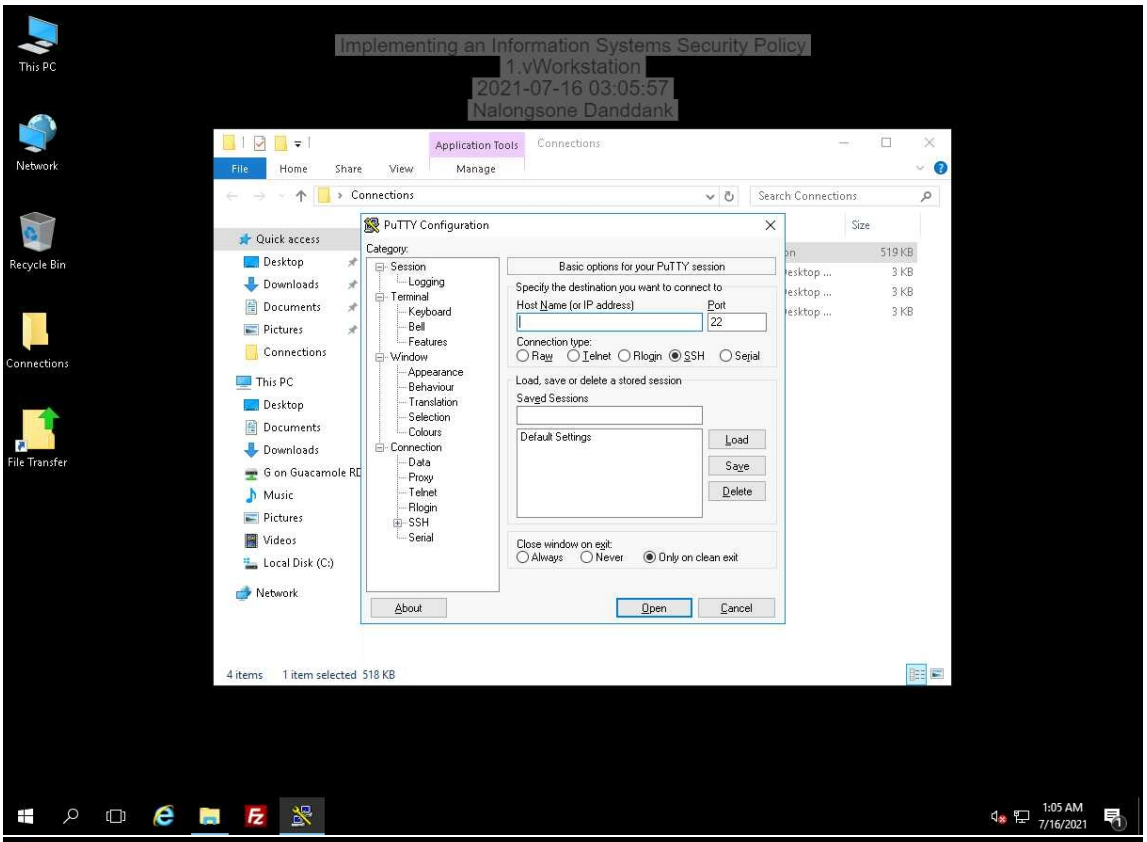

Server Manager
172.30.0.22
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:01:09
Nalongsone Danddank
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
2 Services
Performance
BPA results
7/16/2021 1:00 AM
All Servers 1
Manageability
Events
2 Services
Performance
BPA results
7/16/2021 1:00 AM

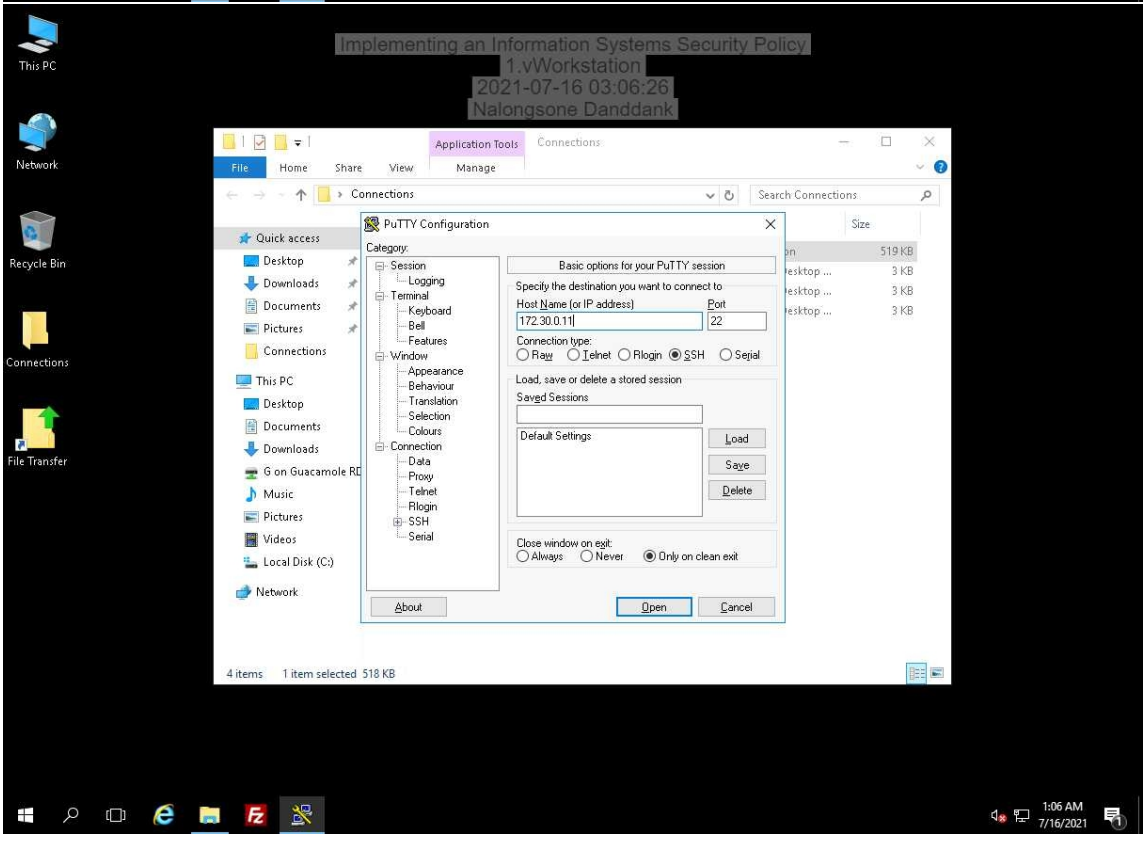

1:01 AM
7/16/2021
172.30.0.22
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:00:52
Nalongsone Danddank
Recycle Bin
1:00 AM
7/16/2021

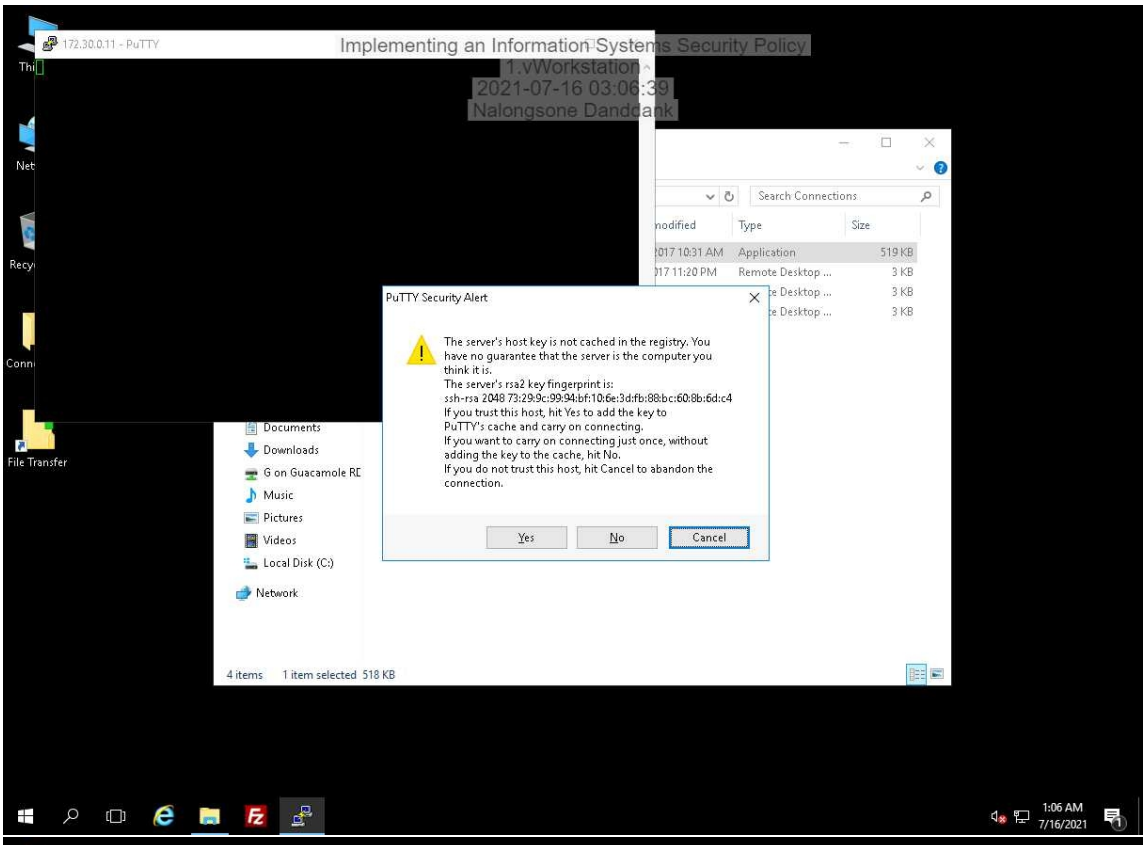


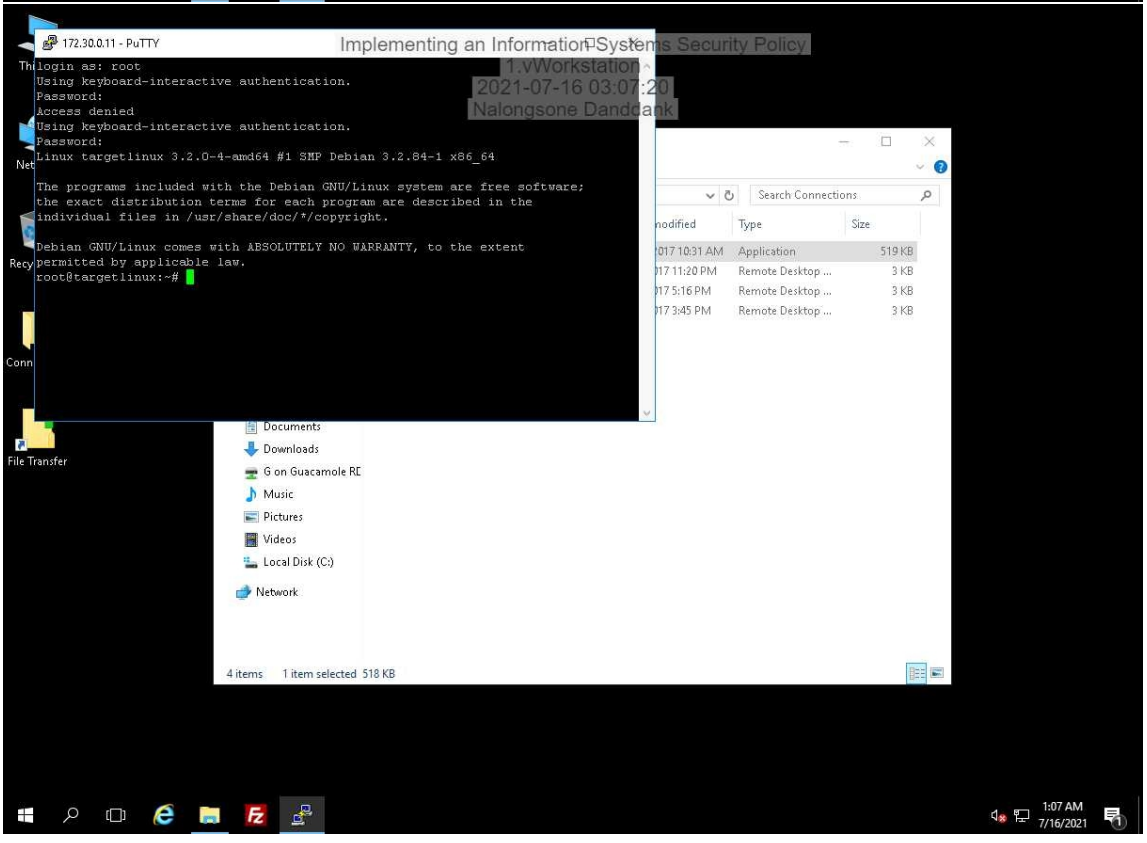
Part 3: Add a Linux Workstation as a member of a Windows Domain.

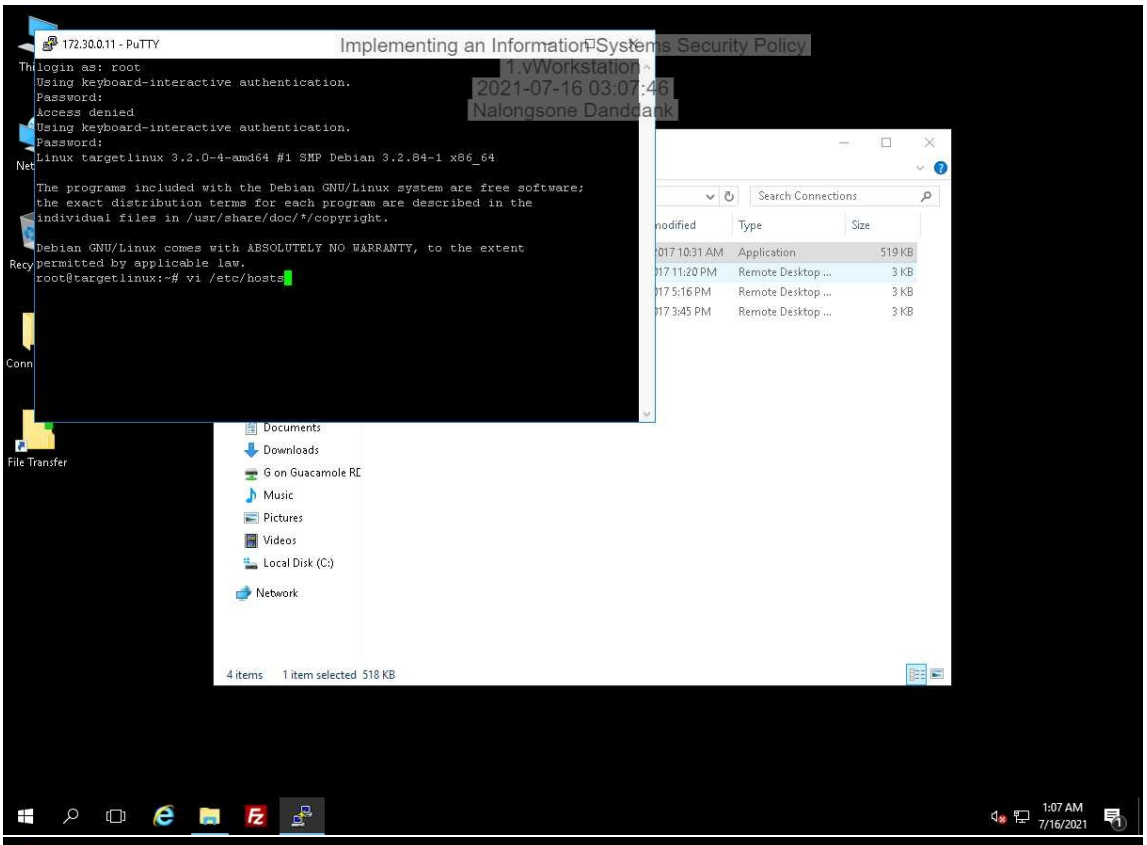


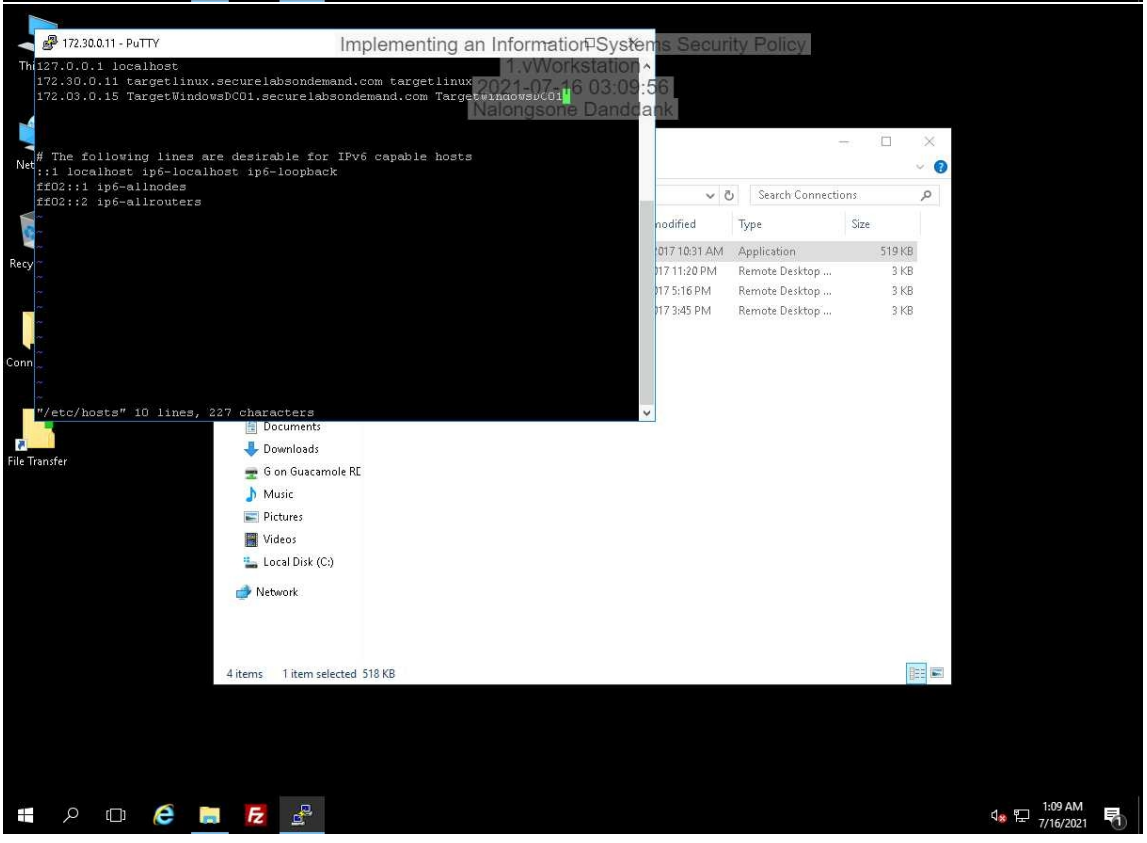

Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:05:57
Nalongsone Danddank
PuTTY Configuration
Host Name (or IP address)
Port
22
Open
Cancel
1:05 AM
7/16/2021

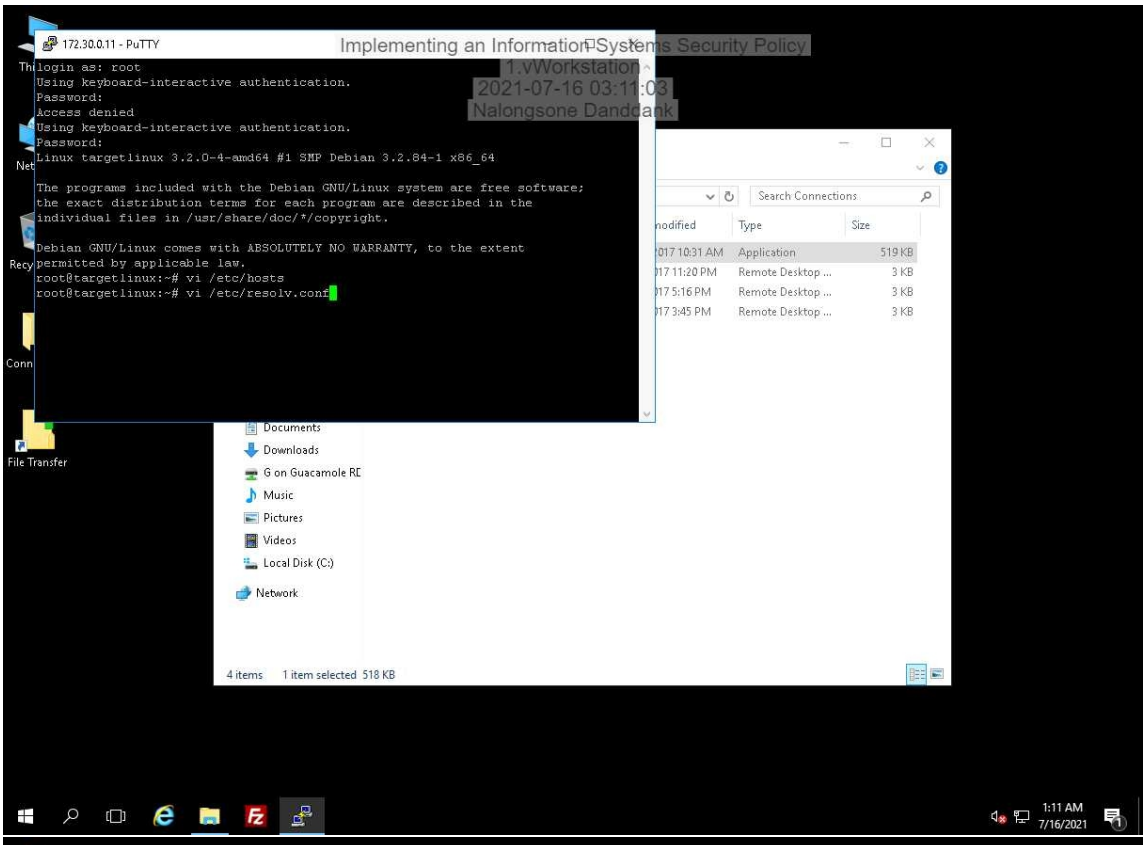

Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:06:26
Nalongsone Danddank
PuTTY Configuration
172.30.0.11
Host Name (or IP address)
Port
22
Open
Cancel
1:06 AM
7/16/2021

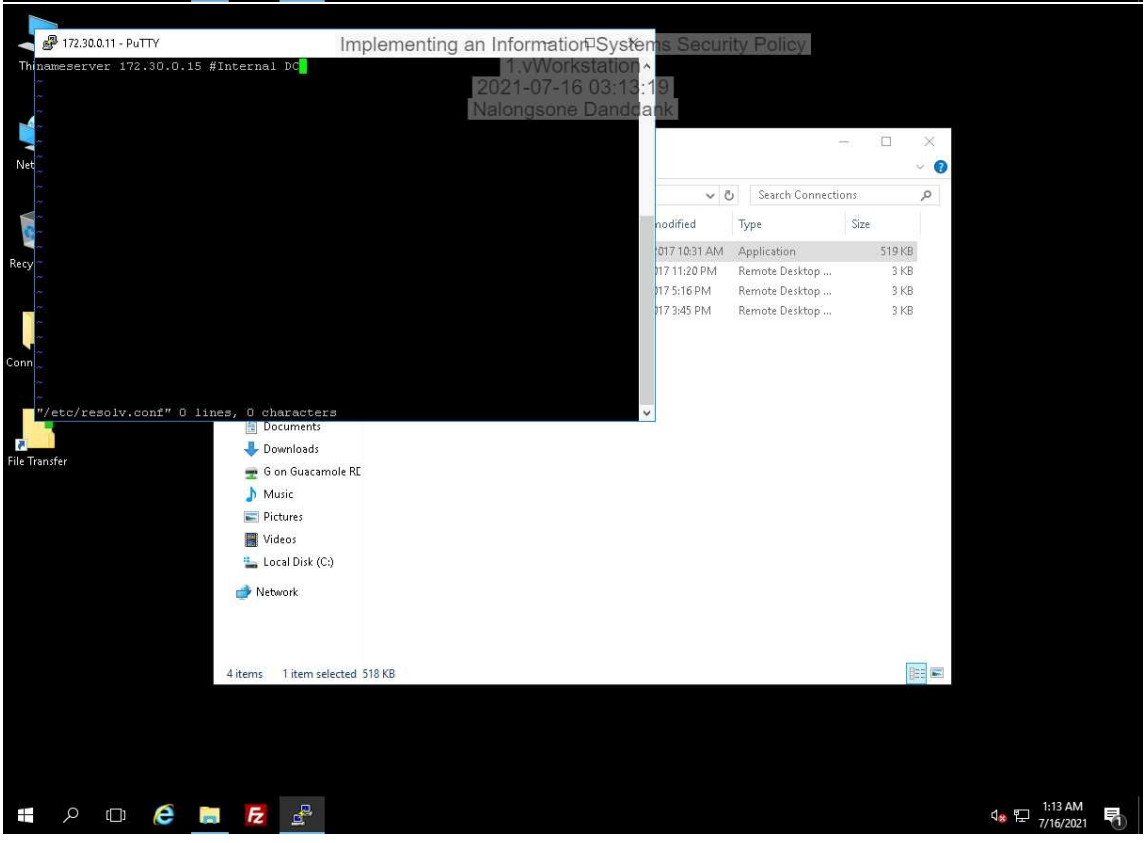

172.30.0.11 - PuTTY
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:06:39
Nalongsone Danddank
PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 73:29:9c:99:94:bf:10:6e:3d:fb:88:bc:60:8b:6d:c4
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes
No
Cancel
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
1:06 AM
7/16/2021

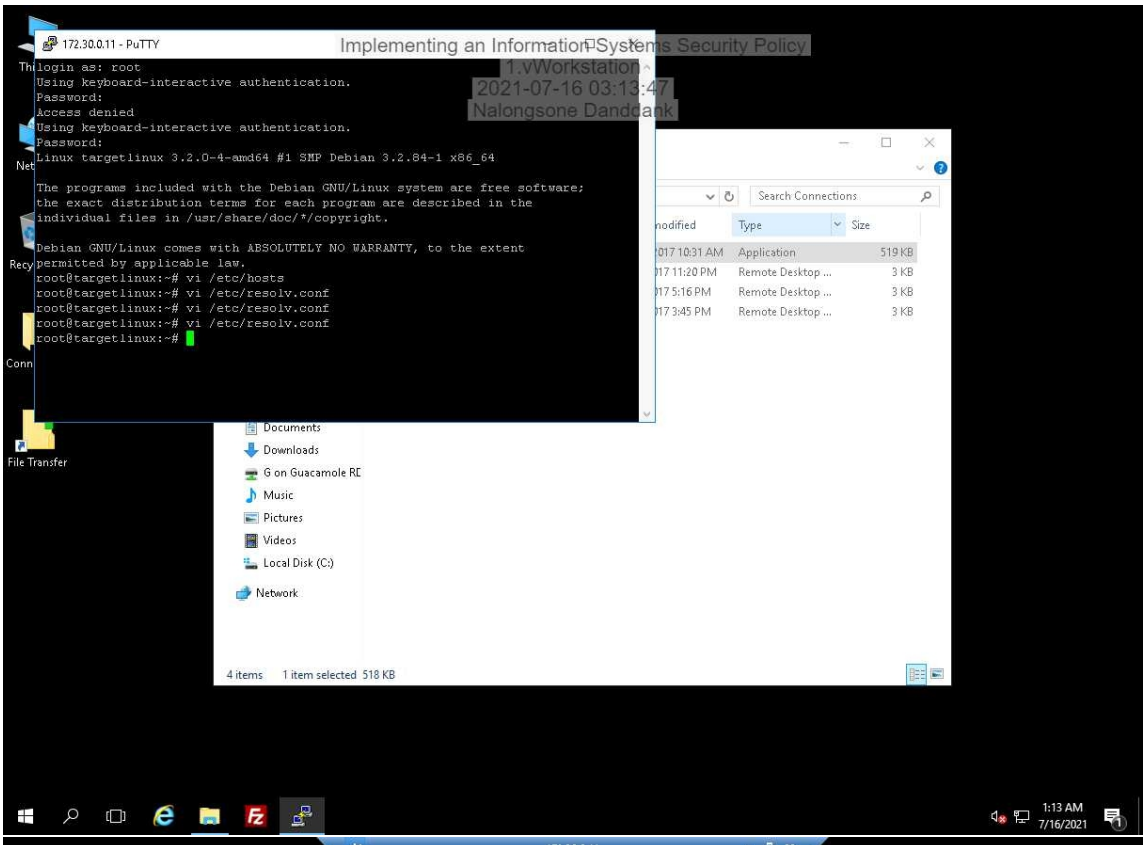

172.30.0.11 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Linux targetlinux 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@targetlinux:~#
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:07:20
Nalongsone Danddank
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
1:07 AM
7/16/2021

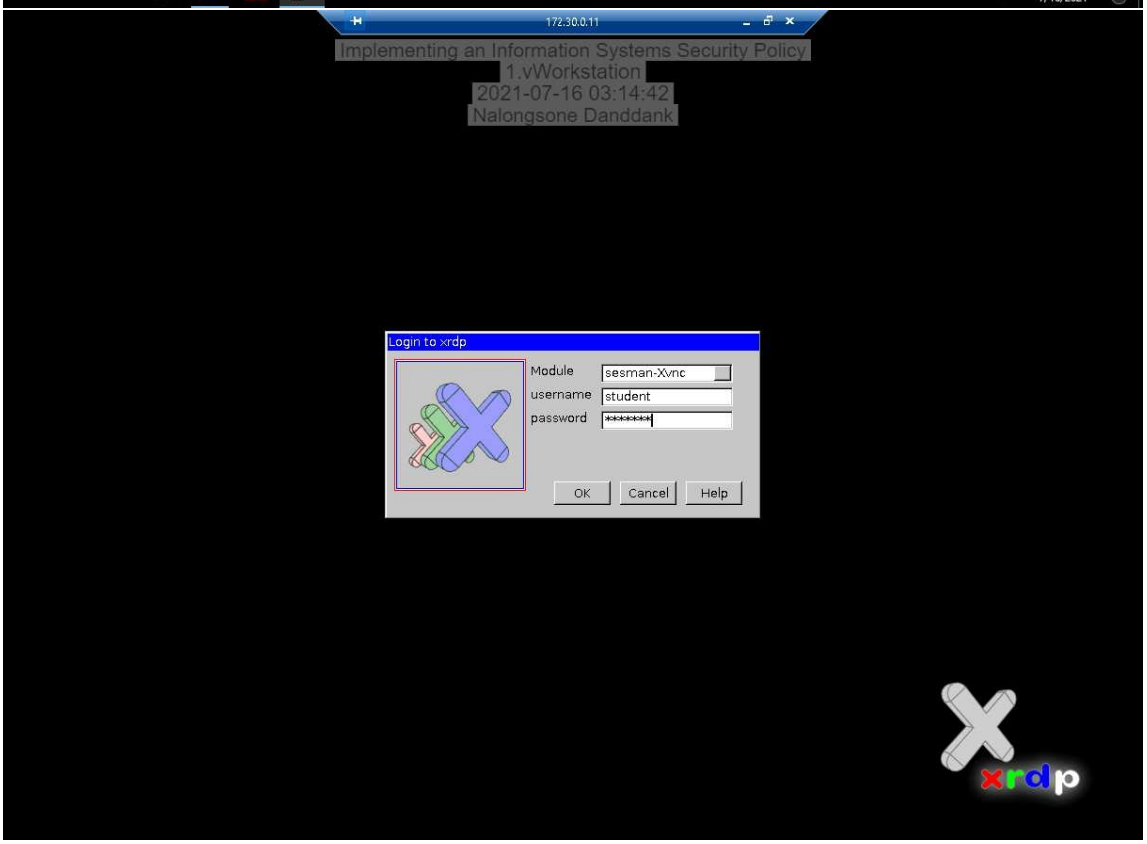

172.30.0.11 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Linux targetlinux 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@targetlinux:~# vi /etc/hosts
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:07:46
Nalongsone Danddank
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
1:07 AM
7/16/2021

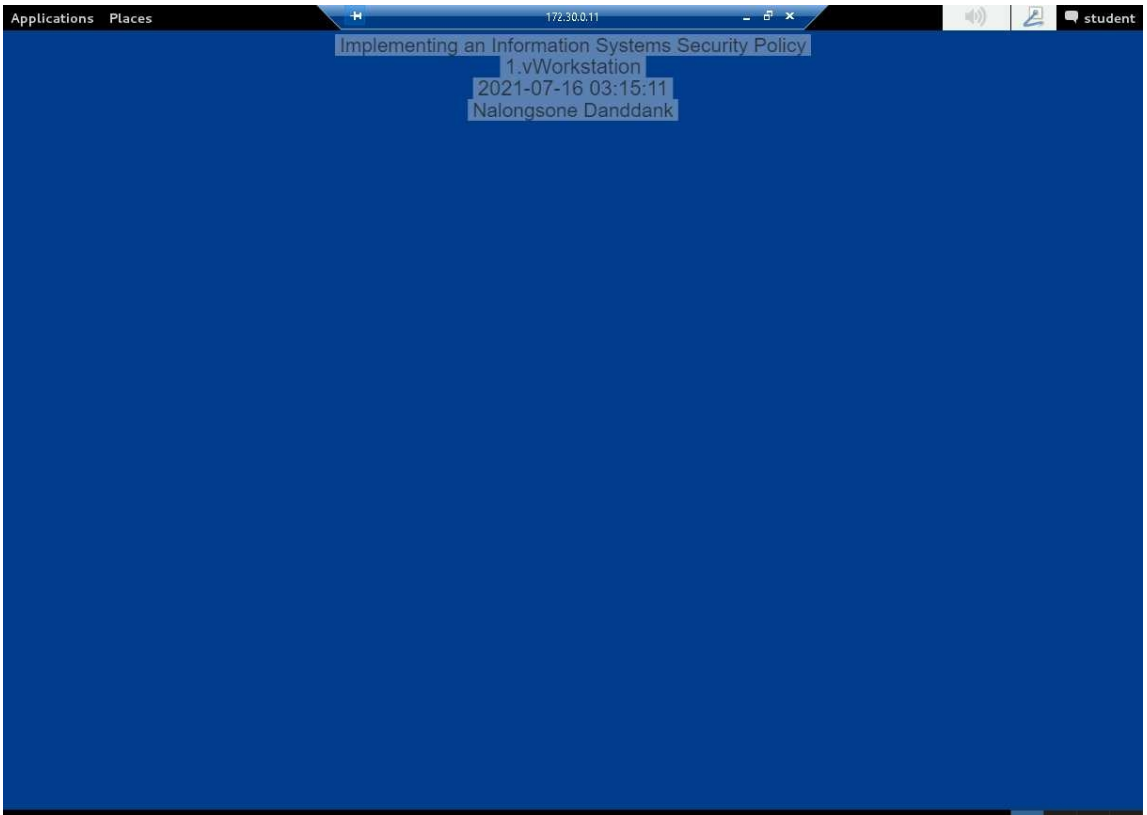

172.30.0.11 - PuTTY
127.0.0.1 localhost
172.30.0.11 targetlinux.securelabsondemand.com targetlinux
172.03.0.15 TargetWindowsDC01.securelabsondemand.com TargetWindowsDC01
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
"/etc/hosts" 10 lines, 227 characters
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:09:56
Nalongsone Danddank
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
1:09 AM
7/16/2021

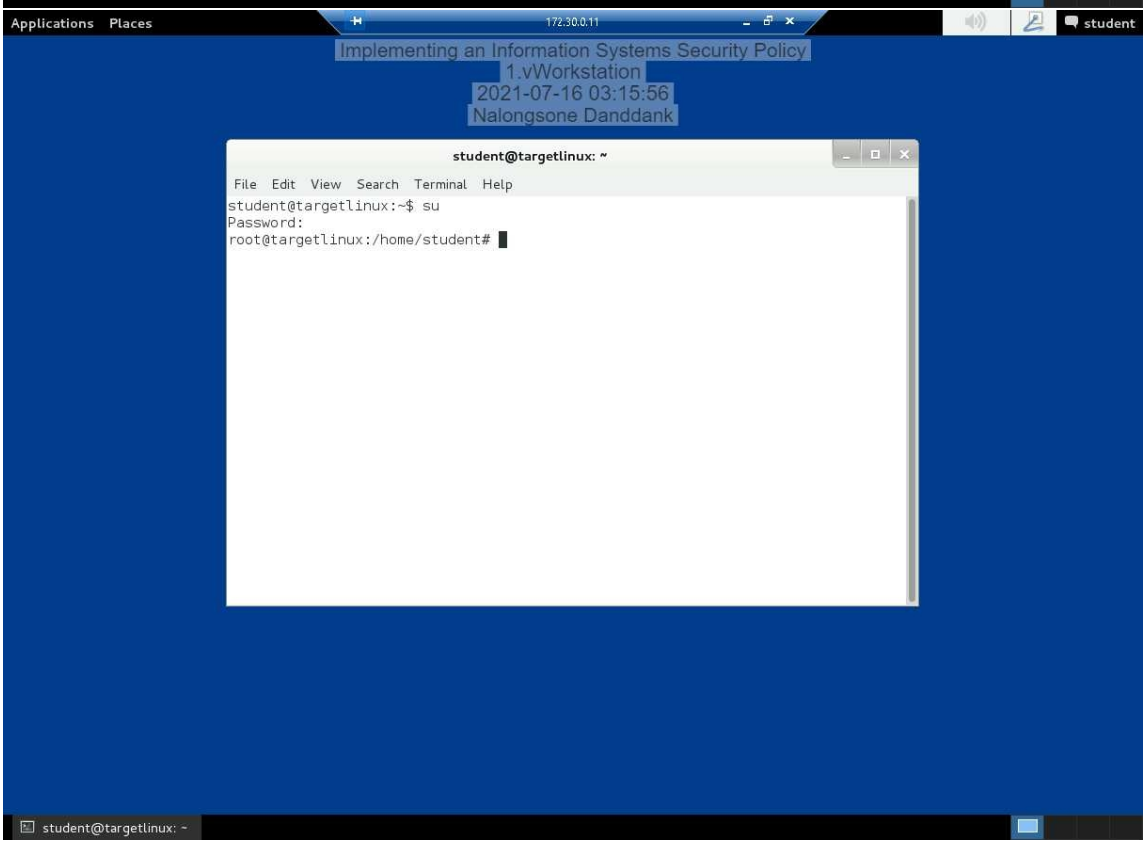

172.30.0.11 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Linux targetlinux 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@targetlinux:~# vi /etc/hosts
root@targetlinux:~# vi /etc/resolv.conf
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:11:03
Nalongsone Danddank
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
1:11 AM
7/16/2021

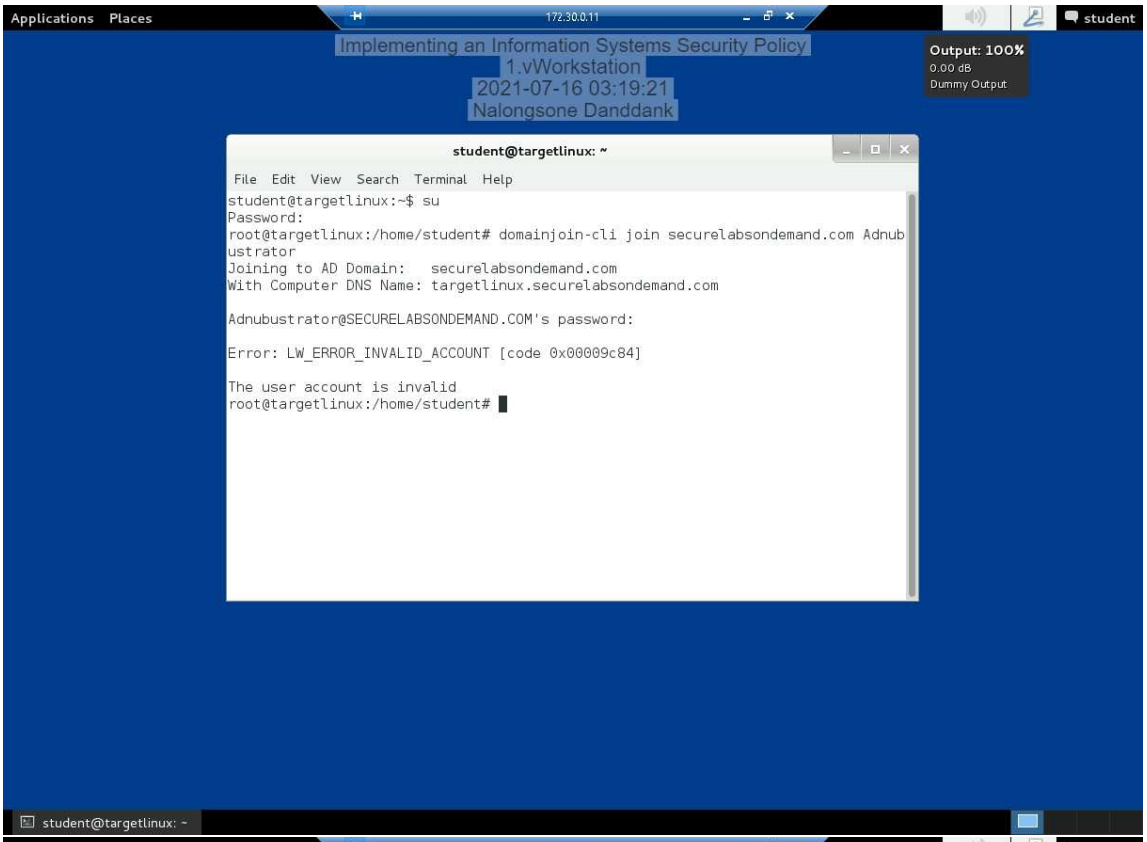

172.30.0.11 - PuTTY
nameserver 172.30.0.15 #Internal DC
"/etc/resolv.conf" 0 lines, 0 characters
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:13:19
Nalongsone Danddank
Search Connections
Type
Size
Application
519 KB
Remote Desktop ...
3 KB
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
1:13 AM
7/16/2021

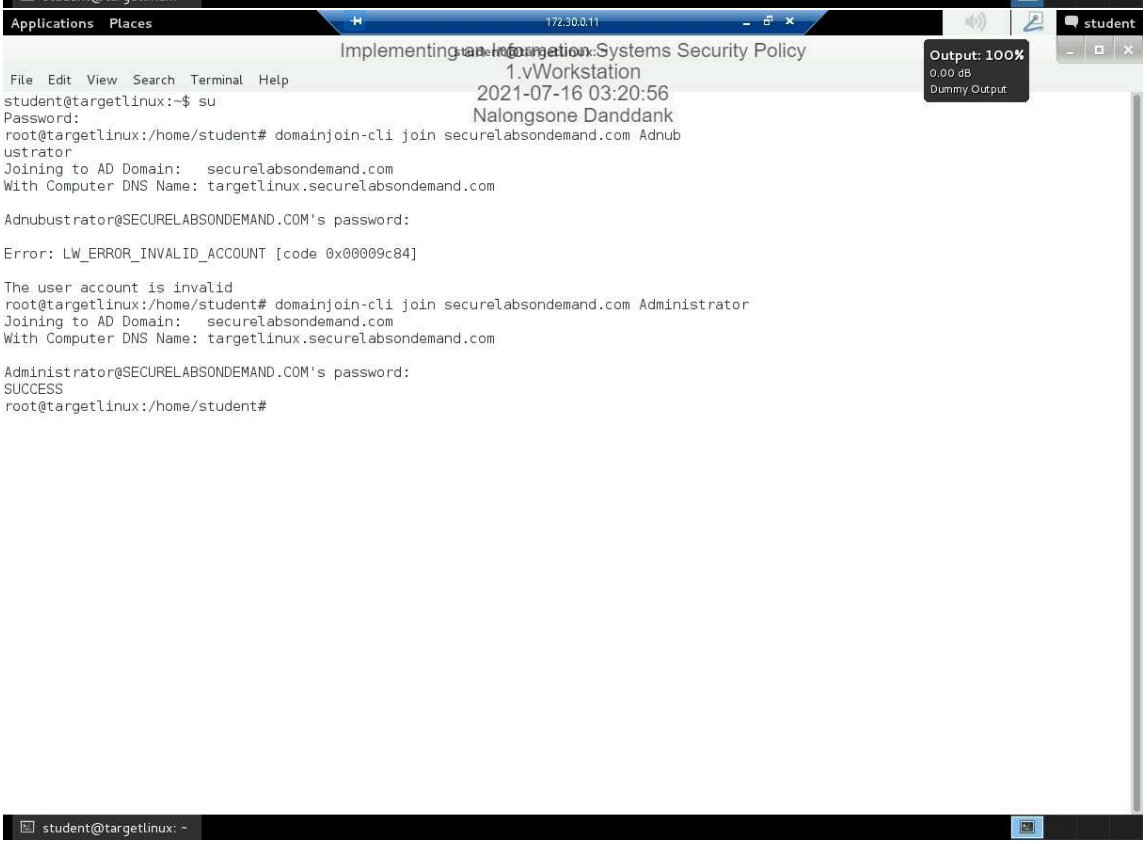

172.30.0.11 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Linux targetlinux 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@targetlinux:~# vi /etc/hosts
root@targetlinux:~# vi /etc/resolv.conf
root@targetlinux:~# vi /etc/resolv.conf
root@targetlinux:~# vi /etc/resolv.conf
root@targetlinux:~#
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:13:47
Nalongsone Danddank
Search Connections
Type
Size
Application 519 KB
Remote Desktop ... 3 KB
Remote Desktop ... 3 KB
Remote Desktop ... 3 KB
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
1:13 AM
7/16/2021

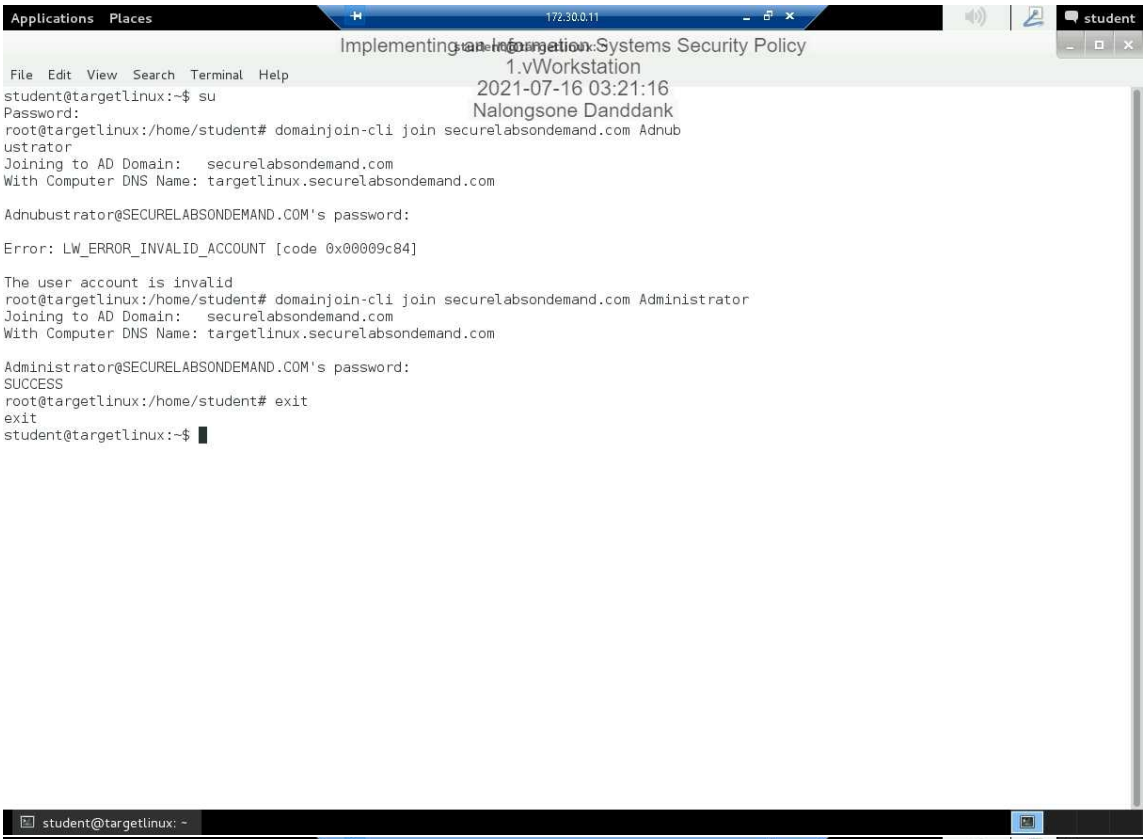

172.30.0.11
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:14:42
Nalongsone Danddank
Login to xrdp
Module
sesman-Xvnc
username
student
password
OK
Cancel
Help
xrdp

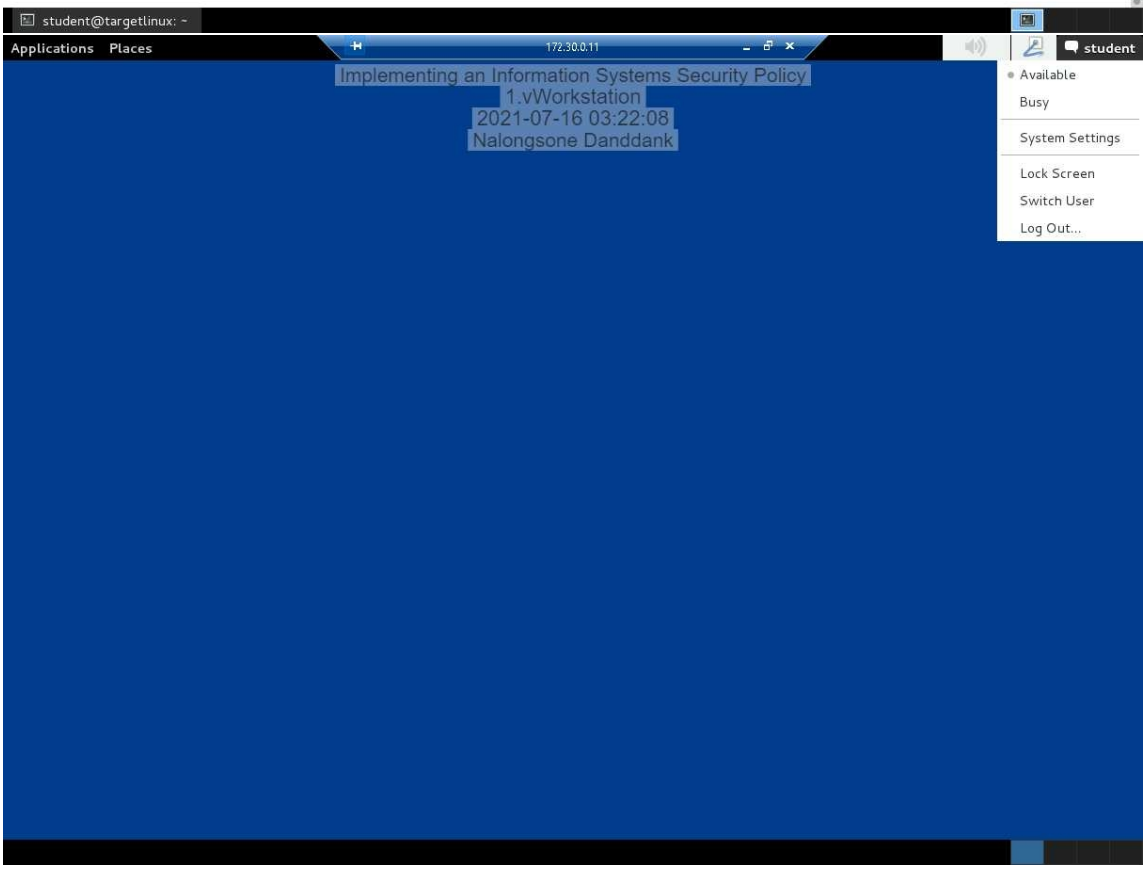

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:15:11
Nalongsone Danddank

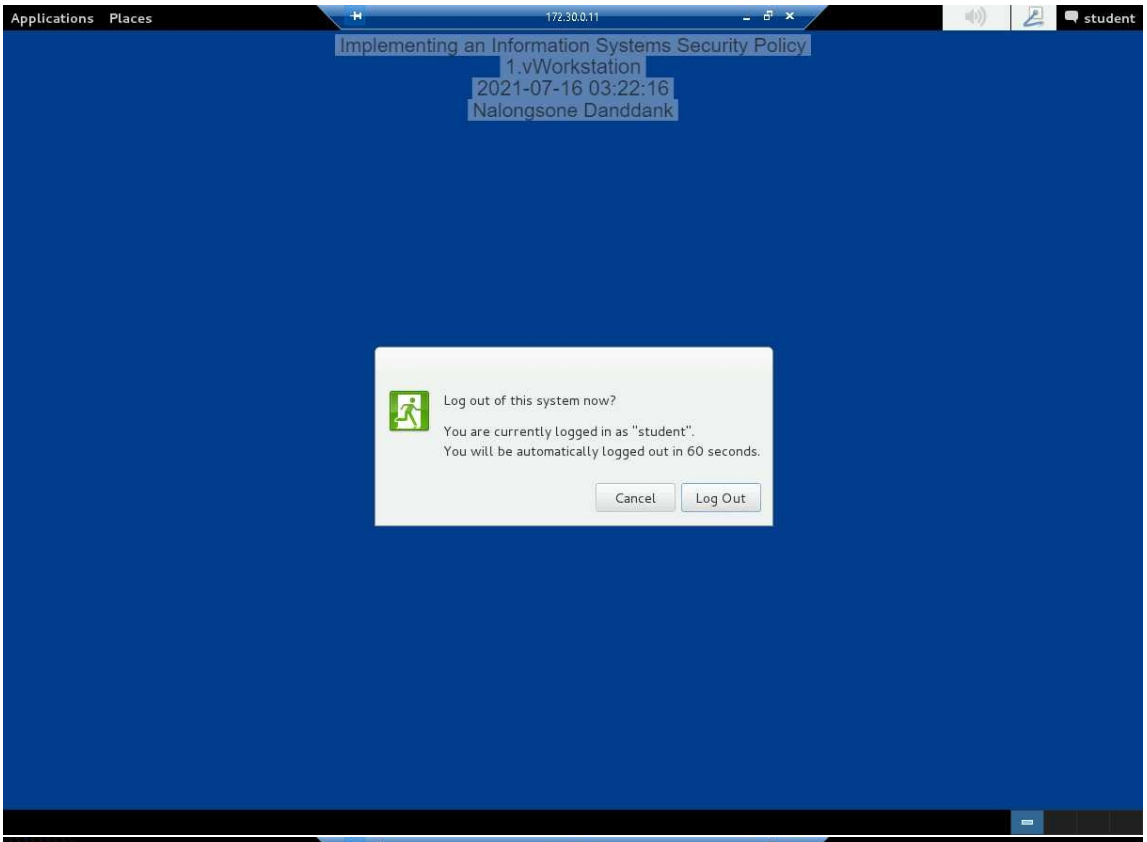

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:15:56
Nalongsone Danddank
student@targetlinux: ~
File Edit View Search Terminal Help
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student#
student@targetlinux: ~

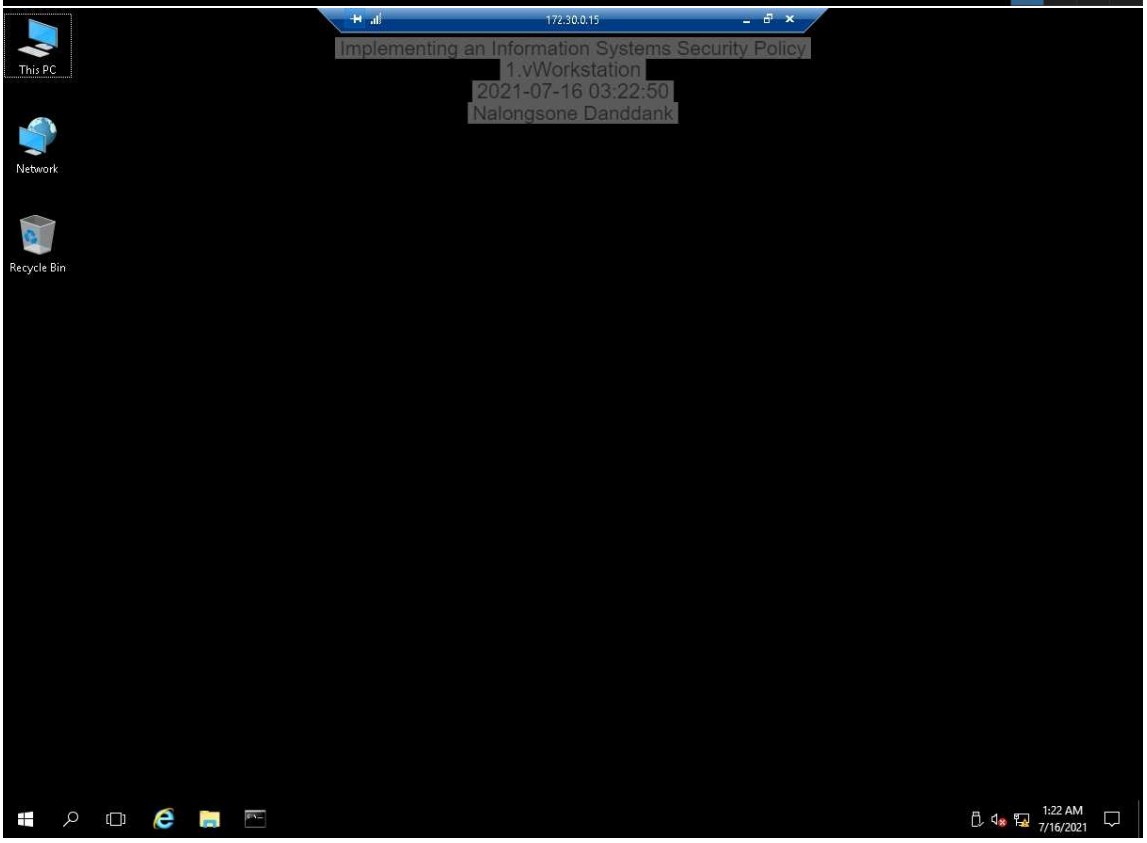

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:19:21
Nalongsone Danddank
Output: 100%
0.00 dB
Dummy Output
student@targetlinux: ~
File Edit View Search Terminal Help
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Adnub
ustrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com
Adnubustrator@SECURELABSONDEMAND.COM's password:
Error: LW_ERROR_INVALID_ACCOUNT [code 0x00009c84]
The user account is invalid
root@targetlinux:/home/student#
student@targetlinux: ~

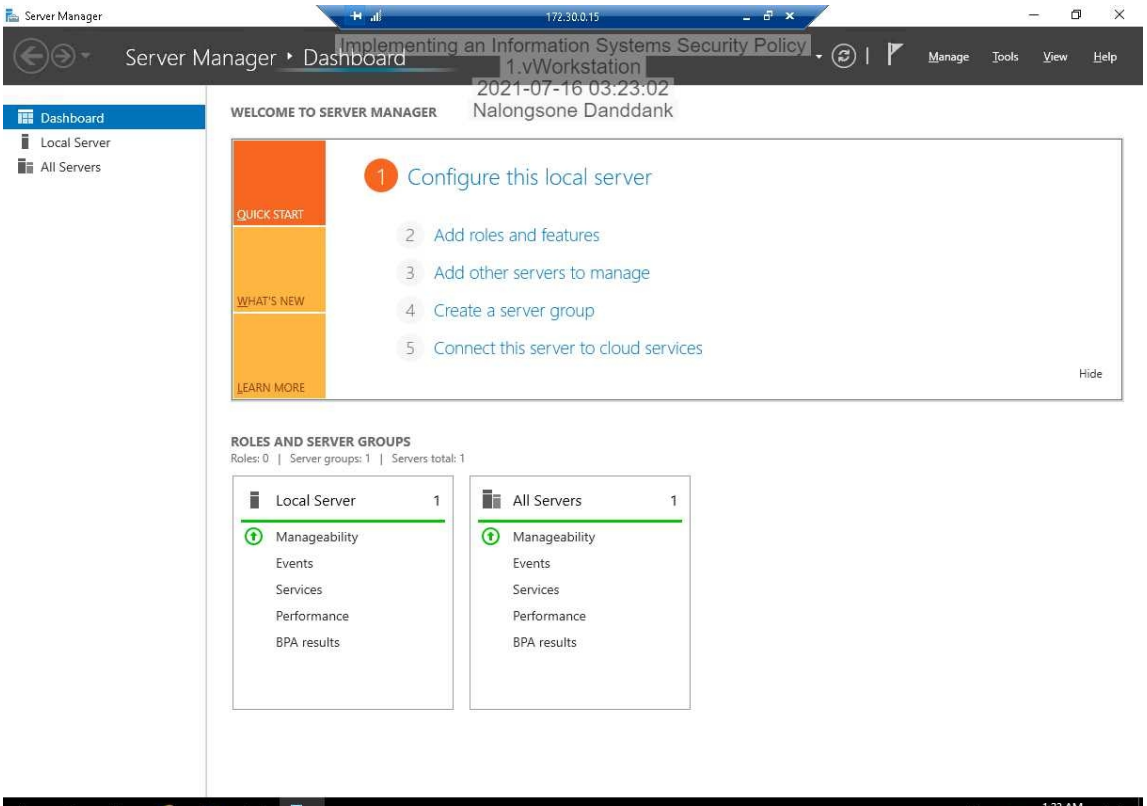

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:20:56
Nalongsone Danddank
Output: 100%
0.00 dB
Dummy Output
File Edit View Search Terminal Help
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Adnub
ustrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com
Adnubustrator@SECURELABSONDEMAND.COM's password:
Error: LW_ERROR_INVALID_ACCOUNT [code 0x00009c84]
The user account is invalid
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Administrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com
Administrator@SECURELABSONDEMAND.COM's password:
SUCCESS
root@targetlinux:/home/student#
student@targetlinux: ~

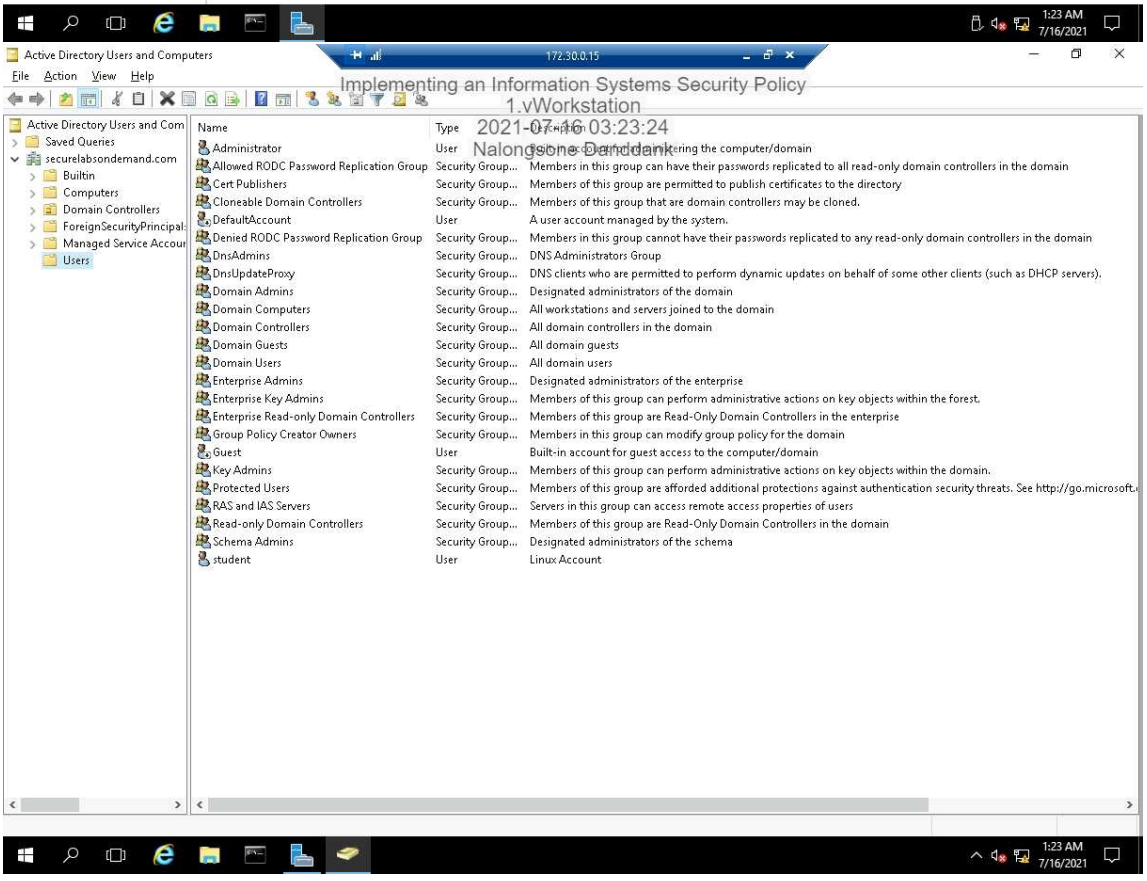

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:21:16
Nalongsone Danddank
File Edit View Search Terminal Help
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Adnub
ustrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com
Adnubustrator@SECURELABSONDEMAND.COM's password:
Error: LW_ERROR_INVALID_ACCOUNT [code 0x00009c84]
The user account is invalid
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Administrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com
Administrator@SECURELABSONDEMAND.COM's password:
SUCCESS
root@targetlinux:/home/student# exit
exit
student@targetlinux:~$

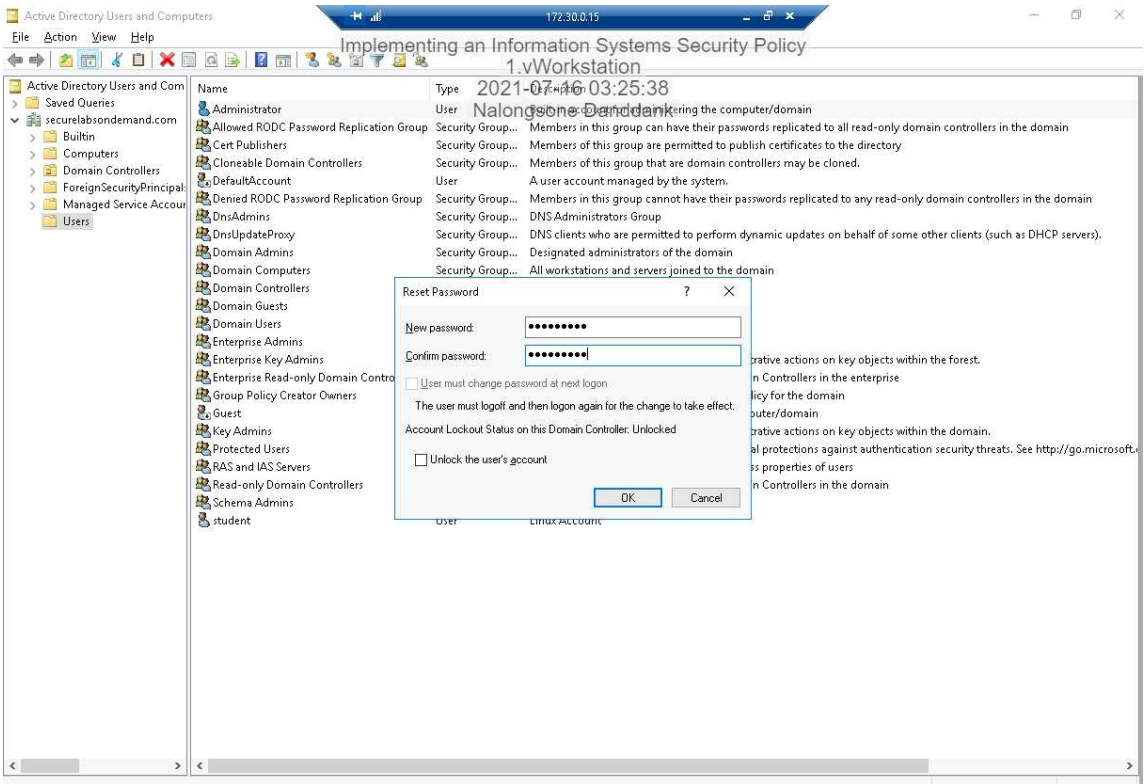

student@targetlinux: ~
Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:22:08
Nalongsone Danddank
Available
Busy
System Settings
Lock Screen
Switch User
Log Out...

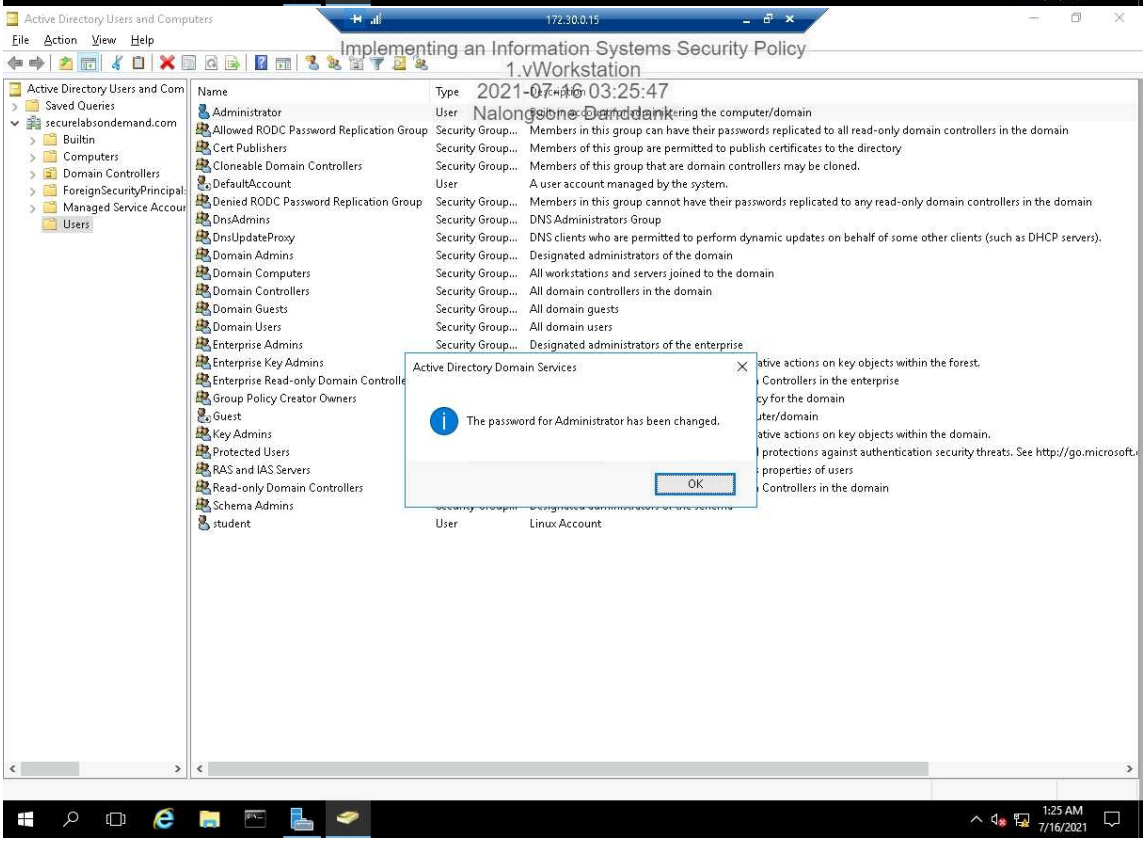

Applications Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:22:16
Nalongsone Danddank
Log out of this system now?
You are currently logged in as "student".
You will be automatically logged out in 60 seconds.
Cancel
Log Out

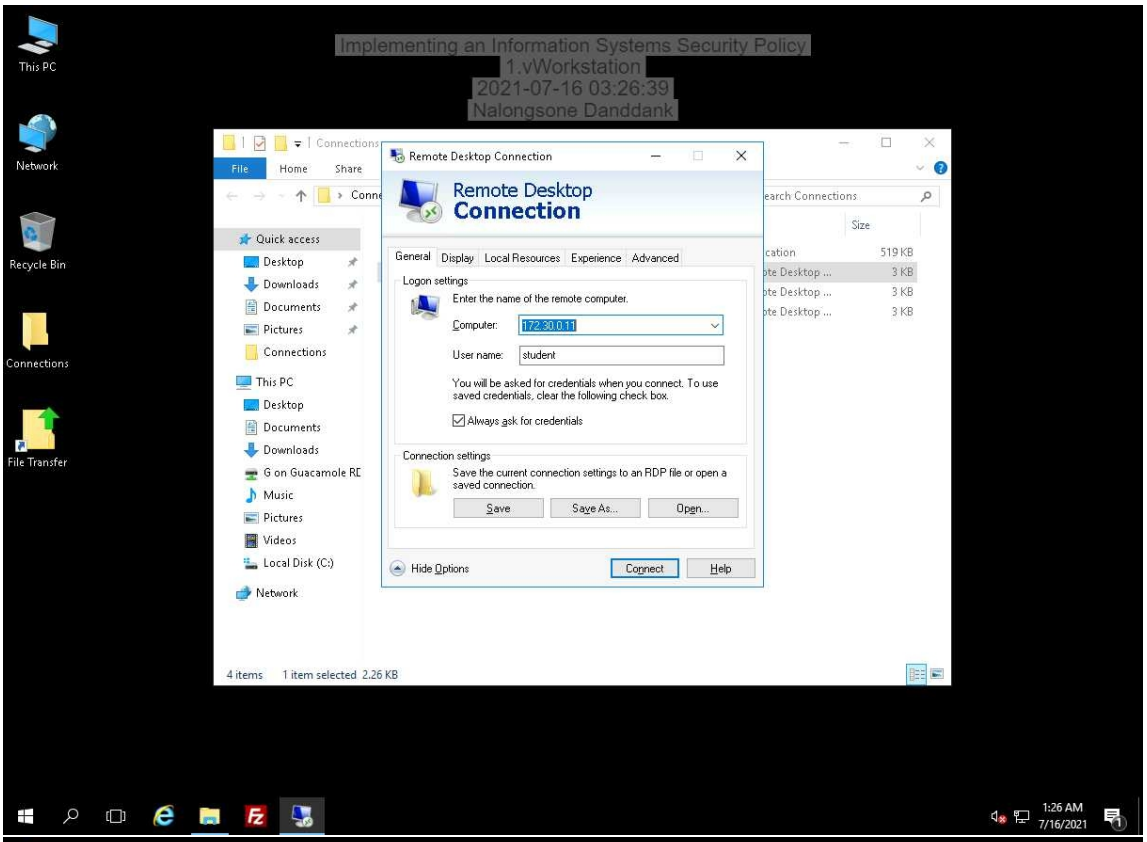

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:22:50
Nalongsone Danddank
This PC
Network
Recycle Bin
1:22 AM
7/16/2021

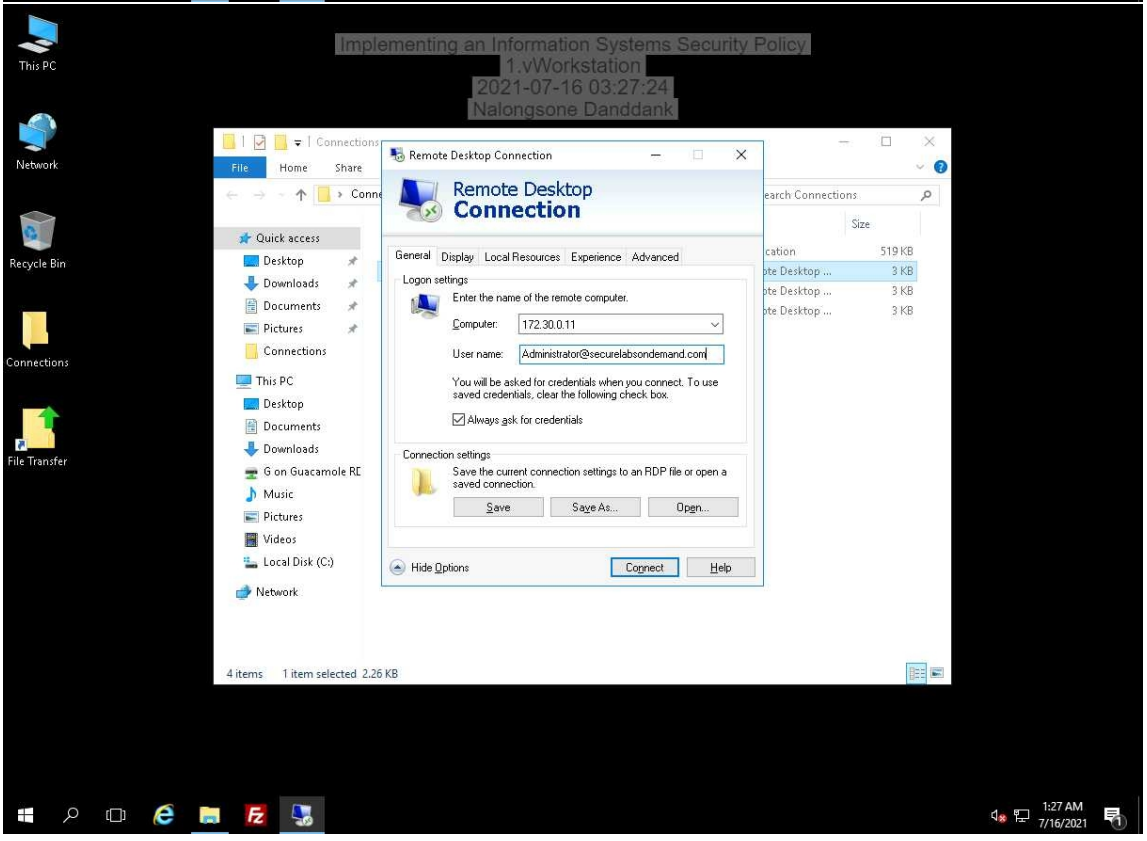

Server Manager
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:23:02
Nalongsone Danddank
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results

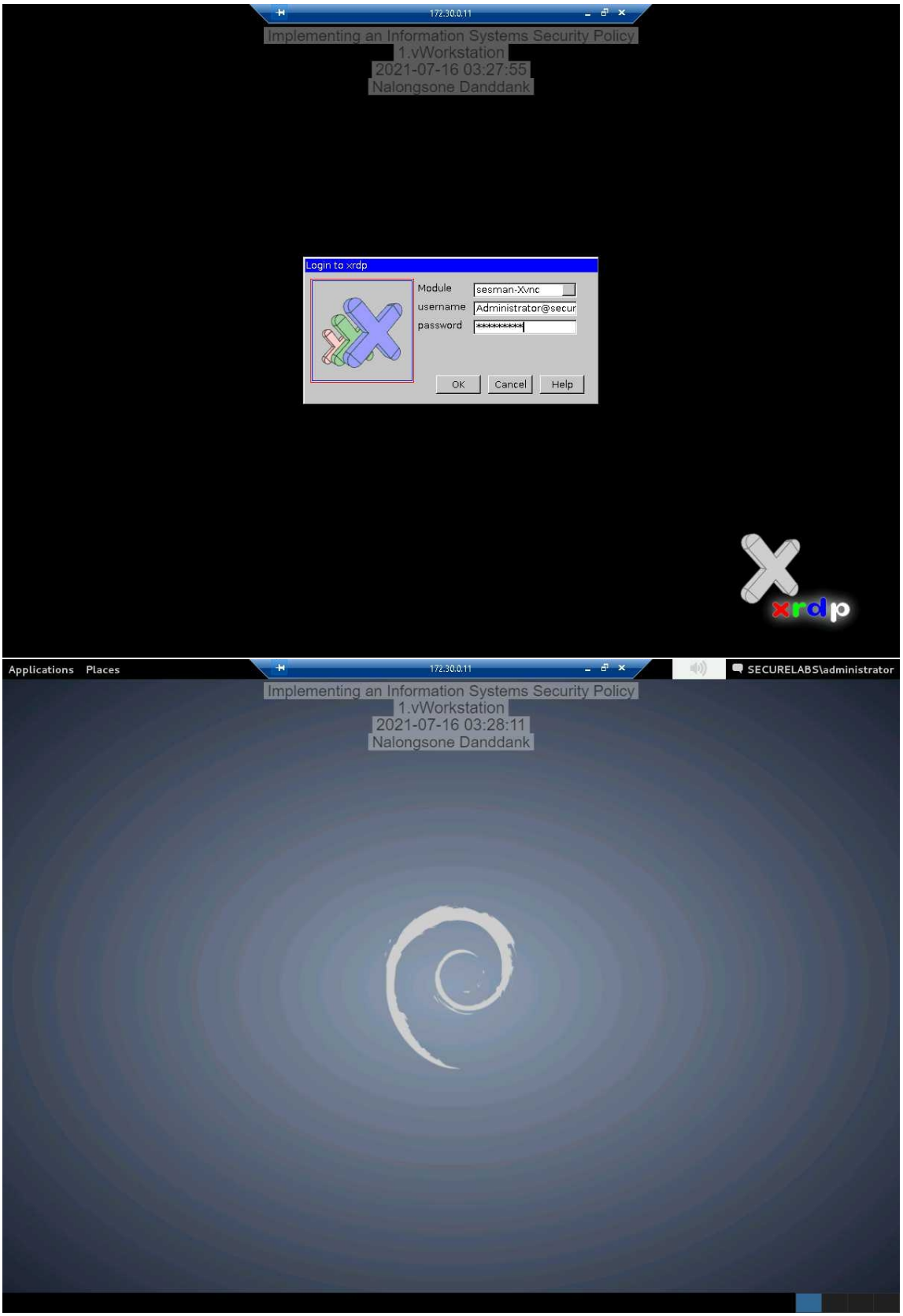

1:23 AM
7/16/2021
Active Directory Users and Computers
172.30.0.15
File Action View Help
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:23:24
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Name Type Description
Administrator User Built-in account for administering the computer/domain
Allowed RODC Password Replication Group Security Group... Members in this group can have their passwords replicated to all read-only domain controllers in the domain
Cert Publishers Security Group... Members of this group are permitted to publish certificates to the directory
Cloneable Domain Controllers Security Group... Members of this group that are domain controllers may be cloned.
DefaultAccount User A user account managed by the system.
Denied RODC Password Replication Group Security Group... Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain
DnsAdmins Security Group... DNS Administrators Group
DnsUpdateProxy Security Group... DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Domain Admins Security Group... Designated administrators of the domain
Domain Computers Security Group... All workstations and servers joined to the domain
Domain Controllers Security Group... All domain controllers in the domain
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise Admins Security Group... Designated administrators of the enterprise
Enterprise Key Admins Security Group... Members of this group can perform administrative actions on key objects within the forest.
Enterprise Read-only Domain Controllers Security Group... Members of this group are Read-Only Domain Controllers in the enterprise
Group Policy Creator Owners Security Group... Members in this group can modify group policy for the domain
Guest User Built-in account for guest access to the computer/domain
Key Admins Security Group... Members of this group can perform administrative actions on key objects within the domain.
Protected Users Security Group... Members of this group are afforded additional protections against authentication security threats. See http://go.microsoft.
RAS and IAS Servers Security Group... Servers in this group can access remote access properties of users
Read-only Domain Controllers Security Group... Members of this group are Read-Only Domain Controllers in the domain
Schema Admins Security Group... Designated administrators of the schema
student User Linux Account
1:23 AM
7/16/2021


Active Directory Users and Computers
172.30.0.15
File Action View Help
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:25:38
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Administrator
Allowed RODC Password Replication Group
Cert Publishers
Cloneable Domain Controllers
DefaultAccount
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Key Admins
Enterprise Read-only Domain Contro
Group Policy Creator Owners
Guest
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
student
Reset Password
New password:
Confirm password:
User must change password at next logon
The user must logoff and then logon again for the change to take effect.
Account Lockout Status on this Domain Controller: Unlocked
Unlock the user's account
OK
Cancel
1:25 AM
7/16/2021


Active Directory Users and Computers
172.30.0.15
File Action View Help
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:25:47
Nalongsone Danddank
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Administrator
Allowed RODC Password Replication Group
Cert Publishers
Cloneable Domain Controllers
DefaultAccount
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Key Admins
Enterprise Read-only Domain Controlle
Group Policy Creator Owners
Guest
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
student
Active Directory Domain Services
The password for Administrator has been changed.
OK
1:25 AM
7/16/2021


Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:26:39
Nalongsone Danddank
Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Logon settings
Enter the name of the remote computer.
Computer:
172.30.0.11
User name:
student
You will be asked for credentials when you connect. To use saved credentials, clear the following check box.
Always ask for credentials
Connection settings
Save the current connection settings to an RDP file or open a saved connection.
Save
Save As...
Open...
Hide Options
Connect
Help
4 items
1 item selected 2.26 KB
1:26 AM
7/16/2021


Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:27:24
Nalongsone Danddank
Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Logon settings
Enter the name of the remote computer.
Computer:
172.30.0.11
User name:
Administrator@securelabsondemand.com
You will be asked for credentials when you connect. To use saved credentials, clear the following check box.
Always ask for credentials
Connection settings
Save the current connection settings to an RDP file or open a saved connection.
Save
Save As...
Open...
Hide Options
Connect
Help
4 items
1 item selected 2.26 KB
1:27 AM
7/16/2021


172.30.0.11
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:27:55
Nalongsone Danddank
Login to xrdp
Module
sesman-Xvnc
username
Administrator@secur
password
OK
Cancel
Help
xrdp
Applications
Places
172.30.0.11
SECURELABS\administrator
Implementing an Information Systems Security Policy
1.vWorkstation
2021-07-16 03:28:11
Nalongsone Danddank

End.