Eric Sosa

Implementing an Information

Systems Security Policy

Lab 10

Section 1: Part 1:

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:02:57
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:03:30
Eric Sosa

Group Policy Management Editor
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:04:55
Eric Sosa
Default Domain Policy [TARGETWINDOWSDC01.SECURE
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (
Preferences
User Configuration
Policies
Preferences
Policy
Policy Setting
Enforce password history
15 passwords remembered
Maximum password age
30 days
Minimum password age
29 days
Minimum password length
7 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Minimum password length Properties
Security Policy Setting
Explain
Minimum password length
Define this policy setting
Password must be at least:
9
characters
OK
Cancel
Apply
4:04 PM
4/7/2021

Group Policy Management Editor
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:05:43
Eric Sosa
Default Domain Policy [TARGETWINDOWSDC01.SECURE
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (
Preferences
User Configuration
Policies
Preferences
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
4:05 PM
4/7/2021

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force_
```

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:06:32
Eric Sosa

User Configuration
Policies
Preferences

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:06:55
Eric Sosa

User Configuration
Policies
Preferences

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:09:26
Eric Sosa
Active Directory Users and Computers [TargetWindow
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
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 Controllers
Group Policy Creator Owners
Guest
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
student
User
Linux Account
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
4:09 PM
4/7/2021

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:10:33
Eric Sosa
Active Directory Users and Computers [TargetWindow
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
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 Controllers
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
4:10 PM
4/7/2021

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:10:50
Eric Sosa
Active Directory Users and Computers [TargetWindow
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
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 Controllers
Group Policy Creator Owners
Guest
Key Admins
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
student
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
4:10 PM
4/7/2021

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:13:56
Eric Sosa
Active Directory Users and Computers [TargetWindow
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
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 Controllers
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 student has been changed.
OK
4:13 PM
4/7/2021

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:15:13
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:15:35
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:16:04
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:16:25
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:17:26
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:18:26
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:19:08
Eric Sosa

Group Policy Management
File Action View Window Help

- 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 | Details | Settings | Delegation

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

4:19 PM 4/7/2021

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 18:20:13
Eric Sosa

Group Policy Management Editor
File Action View Help

- Default Domain Controllers Poli
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Default Domain Controllers Policy [TARGETWINDOWSDC01.SECURELABSONDEMAND.COM] Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration

Extended / Standard

Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
No	Yes	Enabled	None	3/4/2017 3:28:07 PM	securelabsondemand.com

4:20 PM 4/7/2021

Section 1: Part 2:

Section 1: Part 3:

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:07:15
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:07:50
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:08:19
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:08:55
Eric Sosa

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:09:24
Eric Sosa

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
2021-04-07 20:09:54
Eric Sosa

172.30.0.11 - PuTTY

```
127.0.0.1 localhost
172.30.0.11 targetlinux.securelabsondemand.com targetlinux



# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:17:10
Eric Sosa

172.30.0.11 - PuTTY

```
login as: root
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.
Last login: Wed Apr  7 18:08:51 2021 from 172.30.0.2
root@targetlinux:~# vi /etc/hosts
root@targetlinux:~#
```

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:19:04
Eric Sosa

172.30.0.11 - PuTTY

```
login as: root
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.
Last login: Wed Apr  7 18:08:51 2021 from 172.30.0.2
root@targetlinux:~# vi /etc/hosts
root@targetlinux:~# vi /etc/resolv.conf
root@targetlinux:~#
```

Applications Places 172.30.0.11 student

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:19:51
Eric Sosa

Applications Places 172.30.0.11 student

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:21:48
Eric Sosa

student@targetlinux: ~

File Edit View Search Terminal Help

```
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Admin
istrator
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
Close
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:22:40
Eric Sosa
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

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:25:17
Eric Sosa
Active Directory Users and Computers [TargetWindow
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
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 Controllers
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
6:25 PM
4/7/2021

Section 2: Part 1:

Group Policy Management
File Action View Window Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:32:03
Eric Sosa
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 Details Settings Delegation Status
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
6:32 PM
4/7/2021

Group Policy Management Editor
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:32:45
Eric Sosa
Close
Default Domain Policy [TARGET
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [TARGETWINDOWSDC01.SECURELABSONDEMAND.COM] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended Standard
6:32 PM
4/7/2021

Group Policy Management Editor
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:34:36
Eric Sosa
Default Domain Policy [TARGETWINDOWSDC01.SECURELABSC
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECU
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX
Preferences
User Configuration
Policies
Preferences
Policy
Policy Setting
Enforce password history
10 passwords remembered
Maximum password age
25 days
Minimum password age
24 days
Minimum password length
10 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
6:34 PM
4/7/2021

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:36:54
Eric Sosa
Active Directory Users and Com
Saved Queries
securelabsondemand.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
Name
Type
Description
Administrator
User
Built-in account for ad...
Allowed RO...
Security Group...
Members in this group c...
Cert Publish...
Security Group...
Members of this group ...
Cloneable D...
Security Group...
Members of this group t...
DefaultAcco...
User
A user account manage...
Denied ROD...
Security Group...
Members in this group c...
DnsAdmins
Security Group...
DNS Administrators Gro...
DnsUpdateP...
Security Group...
DNS clients who are per...
Domain Ad...
Security Group...
Designated administrato...
Domain Co...
Security Group...
All workstations and ser...
Domain Con...
Security Group...
All domain controllers i...
Domain Gue...
Security Group...
All domain guests
Domain Users
Security Group...
All domain users
Enterprise A...
Security Group...
Designated administrato...
Enterprise K...
Security Group...
Members of this group ...
Enterprise R...
Security Group...
Members of this group ...
Group Polic...
Security Group...
Members in this group c...
Guest
User
Built-in account for gue...
Key Admins
Security Group...
Members of this group ...
Protected Us...
Security Group...
Members of this group ...
RAS and IAS ...
Security Group...
Servers in this group can...
Read-only D...
Security Group...
Members of this group ...
Schema Ad...
Security Group...
Designated administrato...
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
6:36 PM
4/7/2021

Active Directory Users and Computers
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:37:10
Eric Sosa
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 ad...
Allowed RO... Security Group... Members in this group c...
Cert Publish... Security Group... Members of this group ...
Cloneable D... Security Group... Members of this group t...
DefaultAcco... User A user account manage...
Denied ROD... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateP... Security Group... DNS clients who are per...
Domain Ad... Security Group... Designated administrato...
Domain Co... Security Group... All workstations and ser...
Domain Con... Security Group... All domain controllers i...
Domain Gue... Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise A... Security Group... Designated administrato...
Enterprise K... Security Group... Members of this group ...
Enterprise R... Security Group... Members of this group ...
Group Polic... Security Group... Members in this group c...
Guest User Built-in account for gue...
Key Admins Security Group... Members of this group ...
Protected Us... Security Group... Members of this group ...
RAS and IAS ... Security Group... Servers in this group can...
Read-only D... Security Group... Members of this group ...
Schema Ad... Security Group... Designated administrato...
student User Linux Account
Active Directory Domain Services
The password for student has been changed.
OK
6:37 PM
4/7/2021

Group Policy Management Editor
File Action View Help
172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:38:37
Eric Sosa
Default Domain Policy [TARGETWINDOWSDC01.SECURELABSC
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECU
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX
Preferences
User Configuration
Policies
Preferences
Policy Policy Setting
Account lockout duration 5 minutes
Account lockout threshold 3 invalid logon attempts
Reset account lockout counter after 5 minutes
6:38 PM
4/7/2021

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:39:21
Eric Sosa

Group Policy Management Editor

File Action View Help

Default Domain Policy [TARGETWINDOWSDC01.SECURELAI
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active Directory (SI
        - Advanced Audit Policy Configuration
    - Policy-based QoS
  - Administrative Templates: Policy definitions (AD
  - Preferences
- User Configuration
  - Policies
  - Preferences

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

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:39:59
Eric Sosa

Group Policy Management

File Action View Window Help

- 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 | Details | Settings | Delegation | Status

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

Section 2: Part 2:

Section 2: Part 3:

172.30.0.11 - PuTTY
login as: root
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
2021-04-07 20:45:21
Eric Sosa
Connections
Search Connections
Date modified
Type
Size
1/13/2017 10:31 AM
Application
519 KB
2/9/2017 11:20 PM
Remote Desktop ...
3 KB
3/2/2017 5:16 PM
Remote Desktop ...
3 KB
3/4/2017 3:45 PM
Remote Desktop ...
3 KB
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
6:45 PM
4/7/2021

172.30.0.11 - PuTTY
127.0.0.1 localhost
172.30.0.11 targetlinux.securelabsondemand.com targetlinux
172.30.0.15 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
:wq!
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:55:36
Eric Sosa
Connections
Search Connections
Date modified
Type
Size
1/13/2017 10:31 AM
Application
519 KB
2/9/2017 11:20 PM
Remote Desktop ...
3 KB
3/2/2017 5:16 PM
Remote Desktop ...
3 KB
3/4/2017 3:45 PM
Remote Desktop ...
3 KB
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
6:55 PM
4/7/2021

172.30.0.11 - PuTTY
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:56:50
Eric Sosa
login as: root
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
Connections
Search Connections
Date modified
Type
Size
1/13/2017 10:31 AM
Application
519 KB
2/9/2017 11:20 PM
Remote Desktop ...
3 KB
3/2/2017 5:16 PM
Remote Desktop ...
3 KB
3/4/2017 3:45 PM
Remote Desktop ...
3 KB
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
6:56 PM
4/7/2021

172.30.0.11 - PuTTY
nameserver 172.30.0.15 #Internal DC
:wq!
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:58:34
Eric Sosa
Connections
Search Connections
Date modified
Type
Size
1/13/2017 10:31 AM
Application
519 KB
2/9/2017 11:20 PM
Remote Desktop ...
3 KB
3/2/2017 5:16 PM
Remote Desktop ...
3 KB
3/4/2017 3:45 PM
Remote Desktop ...
3 KB
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
6:58 PM
4/7/2021

Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 20:59:17
Eric Sosa
172.30.0.11 - PuTTY
login as: root
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:~# exit
Connections
Search Connections
Date modified
Type
Size
1/13/2017 10:31 AM
Application
519 KB
2/9/2017 11:20 PM
Remote Desktop ...
3 KB
3/2/2017 5:16 PM
Remote Desktop ...
3 KB
3/4/2017 3:45 PM
Remote Desktop ...
3 KB
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
4 items
1 item selected 518 KB
File Transfer
6:59 PM
4/7/2021

Applications
Places
172.30.0.11
student
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 21:00:54
Eric Sosa
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
2021-04-07 21:02:05
Eric Sosa

student@targetlinux: ~

File Edit View Search Terminal Help

```
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Admin
istrator
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
2021-04-07 21:02:44
Eric Sosa

student@targetlinux: ~

File Edit View Search Terminal Help

```
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Admin
istrator
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:~$ exit
```

student@targetlinux: ~

172.30.0.15
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 21:05:15
Eric Sosa
Active Directory Users and Computers
File Action View Help
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 ad...
Allowed RODC Password Replicatio... Security Group... Members in this group c...
Cert Publishers Security Group... Members of this group ...
Cloneable Domain Controllers Security Group... Members of this group t...
DefaultAccount User A user account manage...
Denied RODC Password Replication... 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 Admins Security Group... Members of this group ...
Enterprise Read-only Domain Contr... Security Group... Members of this group ...
Group Policy Creator Owners Security Group... Members in this group c...
Guest User Built-in account for gue...
Key Admins Security Group... Members of this group ...
Protected Users Security Group... Members of this group ...
RAS and IAS Servers Security Group... Servers in this group can...
Read-only Domain Controllers Security Group... Members of this group ...
Schema Admins Security Group... Designated administrato...
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
7:05 PM
4/7/2021

172.30.0.11
Implementing an Information Systems Security Policy
1.vWorkstation
2021-04-07 21:07:06
Eric Sosa
Login to xrdp
Module sesman-Xvnc
username Administrator@secur
password
OK
Cancel
Help
xrdp

Section 3: Part 1:

Analysis and Discussion

In Part 1 of this lab, you changed the Audit Policy to record both successful and unsuccessful login attempts. What drawbacks do you foresee when Auditing is enabled for both success and failure?

One big drawback I noticed right way was that it will be a lot of "events" recorded. Which means if you ever have to go back and search, it will be time consuming.