

Jacen R Kohler

University of North Texas

wINDOWS sERVER Playbook

# Quick Start

This is the 80/20 rule in action. This one page of work will keep out the majority of attacks.

Finish this Quick Start list first, then work through the complete list. Time is of the essence. Red Team is already on the prowl.

Some of these steps will take the computer a while to do. I’ve organized them in a way so you can start one and move onto another while the computer downloads/installs things.

## Security

### Accounts

Ctrl+Alt+Del Change a password…

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Accounts: Rename administrator account = pick something unique

Accounts: Guest account status - Disabled

### Updates

MS03-026, MS08-067, MS08-069, MS09-050, & MS10-025

CMD: wusa [location of .msu] /quiet /warnrestart

### Use Security Configuration Wizard

Start>Administrative Tools>Security Configuration Wizard

### Network security

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Network security: Do not store LAN Manager hash value on next password change = Enabled

Network security: LAN Manager authentication level = Send NTLMv2 response only. refuse NTLM & LM

### Network access

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Network access: Allow anonymous SID/name translation = Disabled

Network access: Do not allow anonymous enumeration of SAM accounts = Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares = Enabled

## Audit Policy

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Audit Policy

Audit process tracking = Success

Audit account management = Success, Failure

Audit logon events = Success, Failure

Audit account logon events = Success, Failure

### User Rights Assignment

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>User Rights Assignment

Debug programs = Remove all groups/users

Allow log on through Terminal/Remote Desktop Services = Leave blank to disallow login via TS even if it has been started.

### Local GOPs

Export a config from a VM or other default install for reference:

CMD: secedit /export /cfg checkme.inf

Edit to to have more secure settings then import onto your target system:

CMD: secedit /configure /db secedit.sdb /cfg securecheckme.inf

Table of Contents

[Quick Start 1](#_Toc474921708)

[Security 1](#_Toc474921709)

[Accounts 1](#_Toc474921710)

[Updates 1](#_Toc474921711)

[Use Security Configuration Wizard 1](#_Toc474921712)

[Network security 1](#_Toc474921713)

[Network access 1](#_Toc474921714)

[Audit Policy 1](#_Toc474921715)

[User Rights Assignment 1](#_Toc474921716)

[Local GOPs 1](#_Toc474921717)

[Complete List 6](#_Toc474921718)

[Updates 6](#_Toc474921719)

[Local Computer Policy 6](#_Toc474921720)

[Windows Settings 6](#_Toc474921721)

[Security Settings 6](#_Toc474921722)

[Account Policies 6](#_Toc474921723)

[Password Policy 6](#_Toc474921724)

[Enforce password history 6](#_Toc474921725)

[Maximum password age 6](#_Toc474921726)

[Minimum password age 6](#_Toc474921727)

[Minimum password length 6](#_Toc474921728)

[Password must meet complexity requirements = Enabled 6](#_Toc474921729)

[Store passwords using reversible encryption = Disabled 6](#_Toc474921730)

[Account Lockout Policy 6](#_Toc474921731)

[Account lockout duration = 5 min 6](#_Toc474921732)

[Account lockout threshold = 3 6](#_Toc474921733)

[Reset account lockout counter after = 5 min 6](#_Toc474921734)

[Local Policies 7](#_Toc474921735)

[Audit Policy 7](#_Toc474921736)

[Audit account logon events = Success, Failure 7](#_Toc474921737)

[Audit account management = Success, Failure 7](#_Toc474921738)

[Audit directory service access = Success, Failure 7](#_Toc474921739)

[Audit logon events = Success, Failure 7](#_Toc474921740)

[Audit object access = Success, Failure 7](#_Toc474921741)

[Audit policy change = Success, Failure 7](#_Toc474921742)

[Audit privilege use = Success, Failure 7](#_Toc474921743)

[Audit process tracking = Success 7](#_Toc474921744)

[Audit system events = Success, Failure 7](#_Toc474921745)

[User Rights Assignment 7](#_Toc474921746)

[Access Credential Manager as a trusted caller = blank 7](#_Toc474921747)

[Access this computer from the network = blank 7](#_Toc474921748)

[Act as part of the operating system = blank 7](#_Toc474921749)

[Add workstations to the domain = blank 7](#_Toc474921750)

[https://technet.microsoft.com/en-us/library/dn221987(v=ws.11).aspx 7](#_Toc474921751)

[Adjust memory quotas for a process = LOCAL SERVICE 7](#_Toc474921752)

[Allow log on locally = Administrators 7](#_Toc474921753)

[Allow log on through Remote Desktop Services = blank 7](#_Toc474921754)

[Backup files and directories = Administrators 7](#_Toc474921755)

[Bypass traverse checking = LOCAL SERVICE 7](#_Toc474921756)

[Change the system time = Administrators 7](#_Toc474921757)

[Change the time zone = Administrators 7](#_Toc474921758)

[Create a pagefile = Administrators 7](#_Toc474921759)

[Create a token object = blank 8](#_Toc474921760)

[Create global objects = LOCAL SERVICE 8](#_Toc474921761)

[Create permanent shared objects = blank 8](#_Toc474921762)

[Create symbolic links = Administrators 8](#_Toc474921763)

[Debug programs = blank 8](#_Toc474921764)

[Deny access to this computer from the network = Guest, ANONYMOUS LOGON, LOCAL SERVICE, NETWORK SERVICE, SERVICE, Local account and member of Administrator group 8](#_Toc474921765)

[Deny log on as a batch job = Guest, ANONYMOUS LOGON 8](#_Toc474921766)

[Deny log on as service = Guest, ANONYMOUS LOGON 8](#_Toc474921767)

[Deny log on locally = Guest, ANONYMOUS LOGON 8](#_Toc474921768)

[Deny log on through Remote Desktop Services = Everyone, ANONYMOUS LOGON 8](#_Toc474921769)

[Enable computer and user accounts to be trusted for delegation = blank 8](#_Toc474921770)

[Force shutdown from a remote system = blank 8](#_Toc474921771)

[Generate security audits = LOCAL SERVICE, Administrators 8](#_Toc474921772)

[Impersonate a client after authentication = Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE 8](#_Toc474921773)

[Increase a process working set = Administrators 8](#_Toc474921774)

[Increase a schedule priority = Administrators 8](#_Toc474921775)

[Load and unload device drivers = blank 8](#_Toc474921776)

[Lock pages in memory = blank 8](#_Toc474921777)

[Log on as batch job = LOCAL SERVICE 8](#_Toc474921778)

[Log on as a service = blank 8](#_Toc474921779)

[Manage auditing and security log = Administrators 8](#_Toc474921780)

[Modify an object label = blank 9](#_Toc474921781)

[Modify firmware environment rules = blank 9](#_Toc474921782)

[Preform volume maintenance tasks = Administrators 9](#_Toc474921783)

[Profile Single Process = Administrators 9](#_Toc474921784)

[Profile system performance = Administrators 9](#_Toc474921785)

[Remove computer from docking station = Administrators 9](#_Toc474921786)

[Replace a process level token = LOCAL SERVICE 9](#_Toc474921787)

[Restore files and directories = Administrators 9](#_Toc474921788)

[Shut down the system = Administrators 9](#_Toc474921789)

[Synchronize directory service data 9](#_Toc474921790)

[Take ownership of files or other objects = Administrators 9](#_Toc474921791)

[Security Options 9](#_Toc474921792)

[Accounts: Administrator account status = Enabled 9](#_Toc474921793)

[Accounts: Block Microsoft accounts = Users can’t add Microsoft accounts 9](#_Toc474921794)

[Accounts: Guest account status = Disabled 9](#_Toc474921795)

[Accounts: Limit local account use of blank passwords to console log on only = Enabled 9](#_Toc474921796)

[Accounts: Rename administrator account = choose something unique 9](#_Toc474921797)

[Accounts: Rename guest account = choose something obvious 9](#_Toc474921798)

[Audit: Audit the access of global system objects = Enabled 9](#_Toc474921799)

[Audit: Audit the use of Backup and Restore privilege = Enabled 10](#_Toc474921800)

[Audit: Force audit policy subcategory settings to override audit policy category settings = Enabled 10](#_Toc474921801)

[Audit: Shut down system immediately if unable to log security audits = Enabled 10](#_Toc474921802)

[DCOM: Machine Access Restrictions in Security Descriptor Definition Language syntax 10](#_Toc474921803)

[DCOM: Machine Launch Restrictions in Security Descriptor Definition Language syntax 10](#_Toc474921804)

[Devices: Allow undock without having to log on = Disabled 10](#_Toc474921805)

[Devices: Allowed to format and eject removable media = Administrators 10](#_Toc474921806)

[Devices: Prevent users from installing printer drivers = Enabled 10](#_Toc474921807)

[Devices: Restrict CD-ROM access to locally logged-on user only = Enabled 10](#_Toc474921808)

[Devices: Restrict floppy access to locally logged-on user only = Enabled 10](#_Toc474921809)

[Domain controller: Allow server operators to schedule tasks = Disabled 10](#_Toc474921810)

[Domain controller: LDAP server signing requirements = Require signing 10](#_Toc474921811)

[Domain controller: Refuse machine account password changes = Enabled 10](#_Toc474921812)

[Domain member: Digitally encrypt or sign secure channel data (always) = Enabled 10](#_Toc474921813)

[Domain member: Digitally encrypt or sign secure channel data (when possible) = Enabled 10](#_Toc474921814)

[Domain member: Digitally sign secure channel data (when possible) = Enabled 10](#_Toc474921815)

[Domain member: Disable machine account password changes = Disabled 10](#_Toc474921816)

[Domain member: Maximum machine account password age = 30 days 10](#_Toc474921817)

[Domain member: Require strong session key = Enabled 10](#_Toc474921818)

[Interactive logon: Display user information when the session is locked = Do not display user information 10](#_Toc474921819)

[Interactive logon: Do not display the last username = Enabled 11](#_Toc474921820)

[Interactive logon: Do not require CTRL+ALT+DEL = Disabled 11](#_Toc474921821)

[Interactive logon: Message text for the users attempting to logon = consult policy handbook 11](#_Toc474921822)

[Interactive logon: Message title for the users attempting to logon = consult policy handbook 11](#_Toc474921823)

[Interactive logon: Number of previous logons to cache = 0 logons 11](#_Toc474921824)

[Interactive logon: Prompt user to change password before expirations = 7 days 11](#_Toc474921825)

[Interactive logon: Require Domain Controller authentication to unlock workstation = Enabled 11](#_Toc474921826)

[Interactive logon: Require smart card = Disabled 11](#_Toc474921827)

[Interactive logon: Smart card removal behavior = Force Logoff 11](#_Toc474921828)

[Microsoft network client: Digitally sign communications (always) = Enabled 11](#_Toc474921829)

[Microsoft network client: Digitally sign communications (if server agrees) = Enabled 11](#_Toc474921830)

[Microsoft network client: Send unencrypted password to third-party SMB servers = Disabled 11](#_Toc474921831)

[Microsoft network server: Amount of idle time required before suspending sessions 5 min 11](#_Toc474921832)

[Microsoft network server: Attempt S4U2Self to obtain claim information = Enabled 11](#_Toc474921833)

[Microsoft network server: Digitally sign communications (always) = Enabled 11](#_Toc474921834)

[Microsoft network server: Digitally sign communications (if client agrees) = Enabled 11](#_Toc474921835)

[Microsoft network server: Disconnect client when logon hours expire = Enabled 11](#_Toc474921836)

[Microsoft network server: Server SPN target name validation level = Required from client 11](#_Toc474921837)

[Network access: Allow anonymous SID/Name translation = Disabled 11](#_Toc474921838)

[Network access: Do not allow anonymous enumeration of SAM accounts = Enabled 11](#_Toc474921839)

[Network access: Do not allow anonymous enumeration of SAM accounts and shares = Enabled 11](#_Toc474921840)

[Network access: Do not allow storage of passwords and credentials for network authentication = Enabled 12](#_Toc474921841)

[Network access: Let Everyone permissions apply to anonymous users = Disabled 12](#_Toc474921842)

[Network access: Named Pipes that can be accessed anonymously = blank 12](#_Toc474921843)

[Network access: Remotely accessible registry paths = blank 12](#_Toc474921844)

[Network access: Remotely accessible registry paths and sub-paths = blank 12](#_Toc474921845)

[Network access: Restrict anonymous access to Named Pipes and Shares = Enabled 12](#_Toc474921846)

[Network access: Shares that can be accessed anonymously = blank 12](#_Toc474921847)

[Network access: Sharing and security model for local accounts = Classic – local users authenticate as themselves 12](#_Toc474921848)

[Network security: Allow local System to use computer identity for NTLM = Enabled 12](#_Toc474921849)

[Network security: Allow localSystem NULL session fallback = Disabled 12](#_Toc474921850)

[Network security: Allow PKU2U authentication requests to this computer to use online identities = Disabled 12](#_Toc474921851)

[Network security: Configure encryption types allowed for Kerberos = AES256\_HMAC\_SHA1 12](#_Toc474921852)

[Network security: Do not store LAN Manager hash value on the next password change = Enabled 12](#_Toc474921853)

[Network security: Force logoff when logon hours expire = Enabled 12](#_Toc474921854)

[Network security: LAN Manager authentication level = Send NTLMv2 response only. refuse NTLM & LM 12](#_Toc474921855)

[Network security: LDAP client signing requirements = Require signing 12](#_Toc474921856)

[Network security: Minimum session security for NTLM SSP based clients = Require 128-bit encryption 12](#_Toc474921857)

[Network security: Minimum session security for NTLM SSP based servers = Require 128-bit encryption 12](#_Toc474921858)

[Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication = blank 13](#_Toc474921859)

[Network security: Restrict NTLM: Add server exceptions in this domain = blank 13](#_Toc474921860)

[Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts 13](#_Toc474921861)

[Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable for domain accounts to domain servers 13](#_Toc474921862)

[Network security: Restrict NTLM: Incoming NTLM traffic = Deny all 13](#_Toc474921863)

[Network security: Restrict NTLM: NTLM authentication in this domain = Deny all 13](#_Toc474921864)

[Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Deny all 13](#_Toc474921865)

[Recovery console: Allow automatic administrative logon = Enable auditing for all accounts 13](#_Toc474921866)

[Recovery console: Allow floppy copy access to all drives and folders = Deisabled 13](#_Toc474921867)

[Shutdown: Allow system to be shut down without having to be logged in = Disabled 13](#_Toc474921868)

[Shutdown: Clear virtual memory pagefile = Enable 13](#_Toc474921869)

[System Cryptography: Force strong key protection for user keys stored on the computer = User must enter a password each time they use a key 13](#_Toc474921870)

[System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing = Enabled 13](#_Toc474921871)

[System objects: Require case insensitivity for non-Windows subsystems = Enabled 13](#_Toc474921872)

[System objects: Strengthen default permissions of internal system objects = Enabled 13](#_Toc474921873)

[System settings: Optional subsystems = NULL 13](#_Toc474921874)

[System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies = Enabled 13](#_Toc474921875)

[User Account Control: Admin Approval Mode for the Built-in Administrator account = Enabled 13](#_Toc474921876)

[User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop = Disabled 14](#_Toc474921877)

[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode = Prompt for credentials on the secure desktop 14](#_Toc474921878)

[User Account Control: Behavior of the elevation prompt for standard users =Prompt for credentials on the secure desktop 14](#_Toc474921879)

[User Account Control: Detect application installations and prompt for elevation = Enabled 14](#_Toc474921880)

[User Account Control: Only elevate executables that are signed and validated = Enabled 14](#_Toc474921881)

[User Account Control: Only elevate UIAccess applications that are installed in secure locations = Enabled 14](#_Toc474921882)

[User Account Control: Run all administrators in Admin Approval Mode = Enabled 14](#_Toc474921883)

[User Account Control: Switch to the secure desktop when prompting for elevation = Enabled 14](#_Toc474921884)

[User Account Control: Virtualize file and registry write failures to per-user locations = Enabled 14](#_Toc474921885)

[Windows Firewall with Advanced Security 14](#_Toc474921886)

[Windows Firewall with Advanced Security 14](#_Toc474921887)

[Network List Manager Policies 14](#_Toc474921888)

[Public Key Policies 14](#_Toc474921889)

[Encrypting File System 14](#_Toc474921890)

[BitLocker Drive Encryption 14](#_Toc474921891)

[Software Restriction Policies 14](#_Toc474921892)

[Application Control Policies 14](#_Toc474921893)

[App Locker 14](#_Toc474921894)

[Executable Rules 14](#_Toc474921895)

[Windows Installer Rules 14](#_Toc474921896)

[Script Rules 14](#_Toc474921897)

[Advanced Audit Policies Configuration 14](#_Toc474921898)

[Advanced Audit Policies – Local Group Policy Object 14](#_Toc474921899)

[Account Logon 15](#_Toc474921900)

[Account Management 15](#_Toc474921901)

[Detailed Tracking 15](#_Toc474921902)

[DS Access 15](#_Toc474921903)

[Logon/Logoff 15](#_Toc474921904)

[Object Access 15](#_Toc474921905)

[Policy Change 15](#_Toc474921906)

[Privilege Use 15](#_Toc474921907)

[System 15](#_Toc474921908)

[Global Access Auditing 15](#_Toc474921909)

[IP Security Policies on Local Computer 15](#_Toc474921910)

[Policy-based QoS 15](#_Toc474921911)

[Administrative Templates 15](#_Toc474921912)

# Complete List

# Updates

<https://support.microsoft.com/en-us/help/934307/description-of-the-windows-update-standalone-installer-in-windows>

Start with the critical ones, then the important ones.

# Local Computer Policy

[GPO\_name]**\Computer Configuration**

## Windows Settings

[GPO\_name]**\Computer Configuration\Windows Settings**

### Security Settings

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings**

#### Account Policies

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Account Policies**

##### Password Policy

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**

<https://technet.microsoft.com/en-us/library/hh994571(v=ws.11).aspx>

https://technet.microsoft.com/en-us/library/hh994572(v=ws.11).aspx

###### Enforce password history

<https://technet.microsoft.com/en-us/library/hh994571(v=ws.11).aspx>

Set **Enforce password history**to 24. This will help mitigate vulnerabilities that are caused by password reuse.

###### Maximum password age

<https://technet.microsoft.com/en-us/library/hh994573(v=ws.11).aspx>

Set Maximum password age to 60 days. Try to expire the passwords between major business cycles to prevent work loss.

###### Minimum password age

<https://technet.microsoft.com/en-us/library/hh994570(v=ws.11).aspx>

Configure Minimum password age so that you do not allow passwords to be changed immediately.

###### Minimum password length

<https://technet.microsoft.com/en-us/library/hh994560(v=ws.11).aspx>

###### Password must meet complexity requirements = Enabled

<https://technet.microsoft.com/en-us/library/hh994562(v=ws.11).aspx>

###### Store passwords using reversible encryption = Disabled

<https://technet.microsoft.com/en-us/library/hh994559(v=ws.11).aspx>

##### Account Lockout Policy

<https://technet.microsoft.com/en-us/library/hh994563(v=ws.11).aspx>

###### Account lockout duration = 5 min

<https://technet.microsoft.com/en-us/library/hh994569(v=ws.11).aspx>

###### Account lockout threshold = 3

<https://technet.microsoft.com/en-us/library/hh994574(v=ws.11).aspx>

###### Reset account lockout counter after = 5 min

<https://technet.microsoft.com/en-us/library/hh994568(v=ws.11).aspx>

#### Local Policies

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Local Policies**

##### Audit Policy

<https://technet.microsoft.com/en-us/library/dd349800(v=ws.10).aspx>

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy**

###### Audit account logon events = Success, Failure

###### Audit account management = Success, Failure

###### Audit directory service access = Success, Failure

###### Audit logon events = Success, Failure

###### Audit object access = Success, Failure

###### Audit policy change = Success, Failure

###### Audit privilege use = Success, Failure

###### Audit process tracking = Success

###### Audit system events = Success, Failure

##### User Rights Assignment

<https://technet.microsoft.com/en-us/library/dn221963(v=ws.11).aspx>

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**

###### Access Credential Manager as a trusted caller = blank

<https://technet.microsoft.com/en-us/library/dn221952(v=ws.11).aspx>

###### Access this computer from the network = blank

<https://technet.microsoft.com/en-us/library/dn221978(v=ws.11).aspx>

###### Act as part of the operating system = blank

<https://technet.microsoft.com/en-us/library/dn221957(v=ws.11).aspx>

###### Add workstations to the domain = blank

###### <https://technet.microsoft.com/en-us/library/dn221987(v=ws.11).aspx>

###### Adjust memory quotas for a process = LOCAL SERVICE

<https://technet.microsoft.com/en-us/library/dn221983(v=ws.11).aspx>

###### Allow log on locally = Administrators

<https://technet.microsoft.com/en-us/library/dn221980(v=ws.11).aspx>

###### Allow log on through Remote Desktop Services = blank

<https://technet.microsoft.com/en-us/library/dn221985(v=ws.11).aspx>

###### Backup files and directories = Administrators

<https://technet.microsoft.com/en-us/library/dn221961(v=ws.11).aspx>

###### Bypass traverse checking = LOCAL SERVICE

<https://technet.microsoft.com/en-us/library/dn221950(v=ws.11).aspx>

###### Change the system time = Administrators

<https://technet.microsoft.com/en-us/library/dn221970(v=ws.11).aspx>

###### Change the time zone = Administrators

<https://technet.microsoft.com/en-us/library/dn221986(v=ws.11).aspx>

###### Create a pagefile = Administrators

<https://technet.microsoft.com/en-us/library/dn221955(v=ws.11).aspx>

###### Create a token object = blank

<https://technet.microsoft.com/en-us/library/dn221946(v=ws.11).aspx>

###### Create global objects = LOCAL SERVICE

<https://technet.microsoft.com/en-us/library/dn221972(v=ws.11).aspx>

###### Create permanent shared objects = blank

<https://technet.microsoft.com/en-us/library/dn221968(v=ws.11).aspx>

###### Create symbolic links = Administrators

<https://technet.microsoft.com/en-us/library/dn221947(v=ws.11).aspx>

###### Debug programs = blank

<https://technet.microsoft.com/en-us/library/dn221969(v=ws.11).aspx>

###### Deny access to this computer from the network = Guest, ANONYMOUS LOGON, LOCAL SERVICE, NETWORK SERVICE, SERVICE, Local account and member of Administrator group

<https://technet.microsoft.com/en-us/library/dn221954(v=ws.11).aspx>

###### Deny log on as a batch job = Guest, ANONYMOUS LOGON

<https://technet.microsoft.com/en-us/library/dn221958(v=ws.11).aspx>

###### Deny log on as service = Guest, ANONYMOUS LOGON

<https://technet.microsoft.com/en-us/library/dn221973(v=ws.11).aspx>

###### Deny log on locally = Guest, ANONYMOUS LOGON

<https://technet.microsoft.com/en-us/library/dn221948(v=ws.11).aspx>

###### Deny log on through Remote Desktop Services = Everyone, ANONYMOUS LOGON

<https://technet.microsoft.com/en-us/library/dn221959(v=ws.11).aspx>

###### Enable computer and user accounts to be trusted for delegation = blank

<https://technet.microsoft.com/en-us/library/dn221977(v=ws.11).aspx>

###### Force shutdown from a remote system = blank

<https://technet.microsoft.com/en-us/library/dn221951(v=ws.11).aspx>

###### Generate security audits = LOCAL SERVICE, Administrators

<https://technet.microsoft.com/en-us/library/dn221956(v=ws.11).aspx>

###### Impersonate a client after authentication = Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE

<https://technet.microsoft.com/en-us/library/dn221967(v=ws.11).aspx>

###### Increase a process working set = Administrators

<https://technet.microsoft.com/en-us/library/dn221949(v=ws.11).aspx>

###### Increase a schedule priority = Administrators

<https://technet.microsoft.com/en-us/library/dn221960(v=ws.11).aspx>

###### Load and unload device drivers = blank

<https://technet.microsoft.com/en-us/library/dn221964(v=ws.11).aspx>

###### Lock pages in memory = blank

<https://technet.microsoft.com/en-us/library/dn221979(v=ws.11).aspx>

###### Log on as batch job = LOCAL SERVICE

<https://technet.microsoft.com/en-us/library/dn221944(v=ws.11).aspx>

###### Log on as a service = blank

<https://technet.microsoft.com/en-us/library/dn221981(v=ws.11).aspx>

###### Manage auditing and security log = Administrators

<https://technet.microsoft.com/en-us/library/dn221953(v=ws.11).aspx>

###### Modify an object label = blank

<https://technet.microsoft.com/en-us/library/dn221974(v=ws.11).aspx>

###### Modify firmware environment rules = blank

<https://technet.microsoft.com/en-us/library/dn221984(v=ws.11).aspx>

###### Preform volume maintenance tasks = Administrators

<https://technet.microsoft.com/en-us/library/dn221971(v=ws.11).aspx>

###### Profile Single Process = Administrators

<https://technet.microsoft.com/en-us/library/dn221982(v=ws.11).aspx>

###### Profile system performance = Administrators

<https://technet.microsoft.com/en-us/library/dn221945(v=ws.11).aspx>

###### Remove computer from docking station = Administrators

<https://technet.microsoft.com/en-us/library/dn221965(v=ws.11).aspx>

###### Replace a process level token = LOCAL SERVICE

<https://technet.microsoft.com/en-us/library/dn221975(v=ws.11).aspx>

###### Restore files and directories = Administrators

<https://technet.microsoft.com/en-us/library/dn221962(v=ws.11).aspx>

###### Shut down the system = Administrators

<https://technet.microsoft.com/en-us/library/dn221966(v=ws.11).aspx>

###### Synchronize directory service data

<https://technet.microsoft.com/en-us/library/dn221988(v=ws.11).aspx>

###### Take ownership of files or other objects = Administrators

<https://technet.microsoft.com/en-us/library/dn221976(v=ws.11).aspx>

##### Security Options

<https://technet.microsoft.com/en-us/library/jj852268(v=ws.11).aspx>

[GPO\_name]**\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

###### Accounts: Administrator account status = Enabled

<https://technet.microsoft.com/en-us/library/jj852165(v=ws.11).aspx>

You will need this to run the server.

###### Accounts: Block Microsoft accounts = Users can’t add Microsoft accounts

<https://technet.microsoft.com/en-us/library/jj966262(v=ws.11).aspx>

###### Accounts: Guest account status = Disabled

<https://technet.microsoft.com/en-us/library/jj852219(v=ws.11).aspx>

Red Team will try to use this for recon and access.

###### Accounts: Limit local account use of blank passwords to console log on only = Enabled

<https://technet.microsoft.com/en-us/library/jj852174(v=ws.11).aspx>

###### Accounts: Rename administrator account = choose something unique

<https://technet.microsoft.com/en-us/library/jj852273(v=ws.11).aspx>

Make it hard for red team have to guess, but easy for you to remember. This will make it harder to brute force.

Examples: Admiral, Akbar, Adamantium

###### Accounts: Rename guest account = choose something obvious

<https://technet.microsoft.com/en-us/library/jj852265(v=ws.11).aspx>

Pick something obvious that will stand out in the logs.

Examples: Imposter, 1337 h4x0r

###### Audit: Audit the access of global system objects = Enabled

<https://technet.microsoft.com/en-us/library/jj852233(v=ws.11).aspx>

###### Audit: Audit the use of Backup and Restore privilege = Enabled

<https://technet.microsoft.com/en-us/library/jj852206(v=ws.11).aspx>

###### Audit: Force audit policy subcategory settings to override audit policy category settings = Enabled

<https://technet.microsoft.com/en-us/library/jj852246(v=ws.11).aspx>

###### Audit: Shut down system immediately if unable to log security audits = Enabled

<https://technet.microsoft.com/en-us/library/jj852263(v=ws.11).aspx>

###### DCOM: Machine Access Restrictions in Security Descriptor Definition Language syntax

<https://technet.microsoft.com/en-us/library/jj852231(v=ws.11).aspx>

Edit Security…>Administrators Local Access

###### DCOM: Machine Launch Restrictions in Security Descriptor Definition Language syntax

<https://technet.microsoft.com/en-us/library/jj852248(v=ws.11).aspx>

Edit Security…>Administrators Local Access

###### Devices: Allow undock without having to log on = Disabled

<https://technet.microsoft.com/en-us/library/jj852203(v=ws.11).aspx>

###### Devices: Allowed to format and eject removable media = Administrators

<https://technet.microsoft.com/en-us/library/jj852171(v=ws.11).aspx>

###### Devices: Prevent users from installing printer drivers = Enabled

<https://technet.microsoft.com/en-us/library/jj852204(v=ws.11).aspx>

###### Devices: Restrict CD-ROM access to locally logged-on user only = Enabled

<https://technet.microsoft.com/en-us/library/jj852279(v=ws.11).aspx>

###### Devices: Restrict floppy access to locally logged-on user only = Enabled

<https://technet.microsoft.com/en-us/library/jj852198(v=ws.11).aspx>

###### Domain controller: Allow server operators to schedule tasks = Disabled

<https://technet.microsoft.com/en-us/library/jj852187(v=ws.11).aspx>

###### Domain controller: LDAP server signing requirements = Require signing

<https://technet.microsoft.com/en-us/library/jj852271(v=ws.11).aspx>

###### Domain controller: Refuse machine account password changes = Enabled

<https://technet.microsoft.com/en-us/library/jj852280(v=ws.11).aspx>

###### Domain member: Digitally encrypt or sign secure channel data (always) = Enabled

<https://technet.microsoft.com/en-us/library/jj852270(v=ws.11).aspx>

###### Domain member: Digitally encrypt or sign secure channel data (when possible) = Enabled

<https://technet.microsoft.com/en-us/library/jj852187(v=ws.11).aspx>

###### Domain member: Digitally sign secure channel data (when possible) = Enabled

<https://technet.microsoft.com/en-us/library/jj852271(v=ws.11).aspx>

###### Domain member: Disable machine account password changes = Disabled

<https://technet.microsoft.com/en-us/library/jj852191(v=ws.11).aspx>

###### Domain member: Maximum machine account password age = 30 days

<https://technet.microsoft.com/en-us/library/jj852252(v=ws.11).aspx>

###### Domain member: Require strong session key = Enabled

<https://technet.microsoft.com/en-us/library/jj852215(v=ws.11).aspx>

###### Interactive logon: Display user information when the session is locked = Do not display user information

<https://technet.microsoft.com/en-us/library/jj852183(v=ws.11).aspx>

###### Interactive logon: Do not display the last username = Enabled

<https://technet.microsoft.com/en-us/library/jj852247(v=ws.11).aspx>

###### Interactive logon: Do not require CTRL+ALT+DEL = Disabled

<https://technet.microsoft.com/en-us/library/jj852250(v=ws.11).aspx>

###### Interactive logon: Message text for the users attempting to logon = consult policy handbook

<https://technet.microsoft.com/en-us/library/jj966264(v=ws.11).aspx>

###### Interactive logon: Message title for the users attempting to logon = consult policy handbook

<https://technet.microsoft.com/en-us/library/jj852182(v=ws.11).aspx>

###### Interactive logon: Number of previous logons to cache = 0 logons

<https://technet.microsoft.com/en-us/library/jj852209(v=ws.11).aspx>

###### Interactive logon: Prompt user to change password before expirations = 7 days

<https://technet.microsoft.com/en-us/library/jj852243(v=ws.11).aspx>

###### Interactive logon: Require Domain Controller authentication to unlock workstation = Enabled

<https://technet.microsoft.com/en-us/library/jj852260(v=ws.11).aspx>

###### Interactive logon: Require smart card = Disabled

<https://technet.microsoft.com/en-us/library/jj852176(v=ws.11).aspx>

###### Interactive logon: Smart card removal behavior = Force Logoff

<https://technet.microsoft.com/en-us/library/jj852235(v=ws.11).aspx>

###### Microsoft network client: Digitally sign communications (always) = Enabled

<https://technet.microsoft.com/en-us/library/jj852186(v=ws.11).aspx>

###### Microsoft network client: Digitally sign communications (if server agrees) = Enabled

<https://technet.microsoft.com/en-us/library/jj852251(v=ws.11).aspx>

###### Microsoft network client: Send unencrypted password to third-party SMB servers = Disabled

<https://technet.microsoft.com/en-us/library/jj852262(v=ws.11).aspx>

###### Microsoft network server: Amount of idle time required before suspending sessions 5 min

<https://technet.microsoft.com/en-us/library/jj852253(v=ws.11).aspx>

###### Microsoft network server: Attempt S4U2Self to obtain claim information = Enabled

<https://technet.microsoft.com/en-us/library/jj966263(v=ws.11).aspx>

###### Microsoft network server: Digitally sign communications (always) = Enabled

<https://technet.microsoft.com/en-us/library/jj852239(v=ws.11).aspx>

###### Microsoft network server: Digitally sign communications (if client agrees) = Enabled

<https://technet.microsoft.com/en-us/library/jj852242(v=ws.11).aspx>

###### Microsoft network server: Disconnect client when logon hours expire = Enabled

<https://technet.microsoft.com/en-us/library/jj852190(v=ws.11).aspx>

###### Microsoft network server: Server SPN target name validation level = Required from client

<https://technet.microsoft.com/en-us/library/jj852272(v=ws.11).aspx>

###### Network access: Allow anonymous SID/Name translation = Disabled

<https://technet.microsoft.com/en-us/library/jj852193(v=ws.11).aspx>

###### Network access: Do not allow anonymous enumeration of SAM accounts = Enabled

<https://technet.microsoft.com/en-us/library/jj852230(v=ws.11).aspx>

###### Network access: Do not allow anonymous enumeration of SAM accounts and shares = Enabled

<https://technet.microsoft.com/en-us/library/jj852184(v=ws.11).aspx>

###### Network access: Do not allow storage of passwords and credentials for network authentication = Enabled

<https://technet.microsoft.com/en-us/library/jj852185(v=ws.11).aspx>

###### Network access: Let Everyone permissions apply to anonymous users = Disabled

<https://technet.microsoft.com/en-us/library/jj852264(v=ws.11).aspx>

###### Network access: Named Pipes that can be accessed anonymously = blank

<https://technet.microsoft.com/en-us/library/jj852278(v=ws.11).aspx>

###### Network access: Remotely accessible registry paths = blank

<https://technet.microsoft.com/en-us/library/jj852177(v=ws.11).aspx>

###### Network access: Remotely accessible registry paths and sub-paths = blank

<https://technet.microsoft.com/en-us/library/jj852237(v=ws.11).aspx>

###### Network access: Restrict anonymous access to Named Pipes and Shares = Enabled

<https://technet.microsoft.com/en-us/library/jj852166(v=ws.11).aspx>

###### Network access: Shares that can be accessed anonymously = blank

<https://technet.microsoft.com/en-us/library/jj852200(v=ws.11).aspx>

###### Network access: Sharing and security model for local accounts = Classic – local users authenticate as themselves

<https://technet.microsoft.com/en-us/library/jj852218(v=ws.11).aspx>

###### Network security: Allow local System to use computer identity for NTLM = Enabled

<https://technet.microsoft.com/en-us/library/jj852275(v=ws.11).aspx>

###### Network security: Allow localSystem NULL session fallback = Disabled

<https://technet.microsoft.com/en-us/library/jj852238(v=ws.11).aspx>

###### Network security: Allow PKU2U authentication requests to this computer to use online identities = Disabled

<https://technet.microsoft.com/en-us/library/jj852232(v=ws.11).aspx>

###### Network security: Configure encryption types allowed for Kerberos = AES256\_HMAC\_SHA1

<https://technet.microsoft.com/en-us/library/jj852180(v=ws.11).aspx>

###### Network security: Do not store LAN Manager hash value on the next password change = Enabled

<https://technet.microsoft.com/en-us/library/jj852276(v=ws.11).aspx>

###### Network security: Force logoff when logon hours expire = Enabled

<https://technet.microsoft.com/en-us/library/jj852195(v=ws.11).aspx>

###### Network security: LAN Manager authentication level = Send NTLMv2 response only. refuse NTLM & LM

<https://technet.microsoft.com/en-us/library/jj852207(v=ws.11).aspx>

###### Network security: LDAP client signing requirements = Require signing

<https://technet.microsoft.com/en-us/library/jj852173(v=ws.11).aspx>

###### Network security: Minimum session security for NTLM SSP based clients = Require 128-bit encryption

<https://technet.microsoft.com/en-us/library/jj852240(v=ws.11).aspx>

###### Network security: Minimum session security for NTLM SSP based servers = Require 128-bit encryption

<https://technet.microsoft.com/en-us/library/jj852194(v=ws.11).aspx>

###### Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication = blank

<https://technet.microsoft.com/en-us/library/jj852269(v=ws.11).aspx>

###### Network security: Restrict NTLM: Add server exceptions in this domain = blank

<https://technet.microsoft.com/en-us/library/jj852267(v=ws.11).aspx>

###### Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts

<https://technet.microsoft.com/en-us/library/jj852175(v=ws.11).aspx>

###### Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable for domain accounts to domain servers

<https://technet.microsoft.com/en-us/library/jj852254(v=ws.11).aspx>

###### Network security: Restrict NTLM: Incoming NTLM traffic = Deny all

<https://technet.microsoft.com/en-us/library/jj852167(v=ws.11).aspx>

###### Network security: Restrict NTLM: NTLM authentication in this domain = Deny all

<https://technet.microsoft.com/en-us/library/jj852241(v=ws.11).aspx>

###### Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Deny all

<https://technet.microsoft.com/en-us/library/jj852213(v=ws.11).aspx>

###### Recovery console: Allow automatic administrative logon = Enable auditing for all accounts

<https://technet.microsoft.com/en-us/library/jj852192(v=ws.11).aspx>

###### Recovery console: Allow floppy copy access to all drives and folders = Deisabled

<https://technet.microsoft.com/en-us/library/jj852208(v=ws.11).aspx>

###### Shutdown: Allow system to be shut down without having to be logged in = Disabled

<https://technet.microsoft.com/en-us/library/jj852274(v=ws.11).aspx>

###### Shutdown: Clear virtual memory pagefile = Enable

<https://technet.microsoft.com/en-us/library/jj852257(v=ws.11).aspx>

###### System Cryptography: Force strong key protection for user keys stored on the computer = User must enter a password each time they use a key

<https://technet.microsoft.com/en-us/library/jj852211(v=ws.11).aspx>

###### System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing = Enabled

<https://technet.microsoft.com/en-us/library/jj852197(v=ws.11).aspx>

###### System objects: Require case insensitivity for non-Windows subsystems = Enabled

<https://technet.microsoft.com/en-us/library/jj852277(v=ws.11).aspx>

###### System objects: Strengthen default permissions of internal system objects = Enabled

<https://technet.microsoft.com/en-us/library/jj852178(v=ws.11).aspx>

###### System settings: Optional subsystems = NULL

<https://technet.microsoft.com/en-us/library/jj852281(v=ws.11).aspx>

###### System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies = Enabled

<https://technet.microsoft.com/en-us/library/jj852261(v=ws.11).aspx>

###### User Account Control: Admin Approval Mode for the Built-in Administrator account = Enabled

<https://technet.microsoft.com/en-us/library/jj852255(v=ws.11).aspx>

###### User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop = Disabled

<https://technet.microsoft.com/en-us/library/jj852245(v=ws.11).aspx>

###### User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode = Prompt for credentials on the secure desktop

<https://technet.microsoft.com/en-us/library/jj852205(v=ws.11).aspx>

###### User Account Control: Behavior of the elevation prompt for standard users =Prompt for credentials on the secure desktop

<https://technet.microsoft.com/en-us/library/jj852259(v=ws.11).aspx>

###### User Account Control: Detect application installations and prompt for elevation = Enabled

<https://technet.microsoft.com/en-us/library/jj852249(v=ws.11).aspx>

###### User Account Control: Only elevate executables that are signed and validated = Enabled

<https://technet.microsoft.com/en-us/library/jj852201(v=ws.11).aspx>

###### User Account Control: Only elevate UIAccess applications that are installed in secure locations = Enabled

<https://technet.microsoft.com/en-us/library/jj852244(v=ws.11).aspx>

###### User Account Control: Run all administrators in Admin Approval Mode = Enabled

<https://technet.microsoft.com/en-us/library/jj852217(v=ws.11).aspx>

###### User Account Control: Switch to the secure desktop when prompting for elevation = Enabled

<https://technet.microsoft.com/en-us/library/jj852236(v=ws.11).aspx>

###### User Account Control: Virtualize file and registry write failures to per-user locations = Enabled

<https://technet.microsoft.com/en-us/library/jj852189(v=ws.11).aspx>

##### Windows Firewall with Advanced Security

###### Windows Firewall with Advanced Security

#### Network List Manager Policies

#### Public Key Policies

##### Encrypting File System

##### BitLocker Drive Encryption

#### Software Restriction Policies

#### Application Control Policies

##### App Locker

###### Executable Rules

###### Windows Installer Rules

###### Script Rules

##### Advanced Audit Policies Configuration

###### Advanced Audit Policies – Local Group Policy Object

<https://technet.microsoft.com/en-us/library/dn452415(v=ws.11).aspx>

Account Logon

Account Management

Detailed Tracking

DS Access

Logon/Logoff

Object Access

Policy Change

Privilege Use

System

Global Access Auditing

#### IP Security Policies on Local Computer

### Policy-based QoS

## Administrative Templates