General Windows

1 Change Passwords
    net user <$uname> {/add, /pword, /delete}
2 Check users
    2.1 AD go through roles
    2.2 SQL go through users and 'browse' basic tables
3 Processes
4 Services
5 Ports
6 Establish primary services
7 Business Injects

Commands:
- Users
  - query user OR TSListUsers
  - net user <$uname> {/add, /pword, /delete}
  - net use
- Services
  - To find them: net start | find "Service Name" OR tasklist
  - To stop them: net stop <exe_name>
  - To kill them: Taskkill /PID <PID> /F
- Aliases
  - Set: doskey <alias>=<command>
  - List: set
  - Delete (set blank): doskey <alias>=<nothing>
- grep == findstr
- net user guest /active:no
- net share {/delete, /create} <filename>

Tools/Downloads:
- Start msconfig.exe
- Microsoft SQL Server 2008 has best compatibility with win 2003r2 Service Pack 2
- In cmd:
  - color 0f <zero> <f>
  - echo off/on
- Google "Security Update for Windows <year>"

Procedures:
- Shared folder:
  - Creat new folder -> "share with" button ->specify people -> "Everyone" -> "Add" -> "Share" -> "Done" THEN Admin Tools (from start menu) -> Computer Management -> Expand "Shared Folders" -> "Shares" -> Properties -> Publish Tabs -> check "Publish this…" -> Edit -> Add testing

- Search in AD
  - Start->Network->"Search AD"
- DNS
  - After installed role -> Open DNS manager -> On left side, Expand AD -> R-click Forward Lookup Zone -> new zone -> teamfsu.local -> next -> Do not allow dynamic updates -> Finish
- SQL

Enable Force Protocol Encryption and Trust Server Cert. Click Start -> All programs -> Microsoft SQL Server 2008 -> Config Tools -> SQL server Config Manager ->SQL Native Client (Right click and access properties) -> Enable FPE and Trust Server Cert. (These changes will be implemented on restart, I recommend finishing any other changes before restarting)

Check for Aliases in SQL Server Config Manager under SQL Natice Client 10.0 Config

Enable Filestream for Transact SQL access. In SQL server config manger click SQL server services -> Click FILESTREAM -> Enable Filestream for Transact SQL

Remote MMC

1. Firewall Snap-in

netsh advfirewall firewall set rule group= "Windows Firewall Remote Management" new enable = yes

Any MMC Snao-in

netsh advfirewall firewall set rule group ="Remote Administration new enable =yes

1. Services Snap-in Snap-in

netsh advfirewall firewall set rule group ="Remote Service Management" new enable =yes

2. Disk Management Snap-in

sc start vds

sc config vds start auto

3. IP Security Policy Management Snap-in

cscript %windir%\system32\scregedit /im 1

To access from another Windows Machine or use the Remote MMC Application:

cmdkey /add:<servername> /user:<username> /pass:<password>

Remote Desktop

netsh advfirewall firewall set rule group="remote desktop" new enable=no

- Enable=0, Disable=1, check= /ar /v cscript %windiF/,\system32\scregedit.wsf /ar 1

net user guest /active:no

netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=na

Firewall - http://support.microsoft.com/kb/947709

- Enable: netsh advfirewall set currentprofile state on
- netsh advfirewall set currentprofile firewallpolicy blockinboundalways,allowoutbound
- Reset: netsh advfirewall reset
- Enable Specific Port: netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80
- Enable Specific Program: netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable =yes
- remoteipz157.60.0.1,172.16.0.0/1 6,LocalSubnet profile= domain
- Logging: netsh firewall set logging %systemroot%\system32\LogFiles\Firewall\pfirewall.log 4096 ENABLE ENABLE
- Delete Program: netsh advfirewall firewall delete rule name="rulename"
- Program="C :\MVApp\MyApp.exe
- Delete Port: netsh advfirewall firewall delete rule name="rulename" protocol=udp
- Localport = 500
- Enable Ping: netsh advfirewall firewall add rule name;"lCMP Allow incoming V4 echo
- Request" protocol =icmpv 4:8 ,any dir = in action =allow
- Netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80
- Netsh advfirewall firewall add rule name="File and Printer Sharing" new enable=no
- Netsh firewall set logging %systemroot%\system32\LogFiles\Firewall\pfirewall.log 4096 ENABLE ENABLE
- Enable ping: netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow

General Windows Checklist (V2)

For workstations, unplug ethernet cable until you begin running windows updates
Never leave remote desktop open and unattended.

1 . Change Passwords, rename admin accounts, deactivate default accounts
- wmic useraccount where named ='currentname' rename newname
- net used '<username>'
- net user <username> /active:no
  - net user guest /active:no
  - net user administrator /active:yes
- Force Password Reset on Domain Users
- Enable windows firewall

2. Disable Network sharing and remove shared folders
4. Disable unneeded services msconfig, Servcies.msc
5. Uninstall unneeded software
6. Enable auditing on "Documents" and "Windows" folders (gpedit-)audit, then select
- auditing in specific folders)
- Audit process tracking - Successes
- Audit account management - Successes, Failures
- Audit logon events - Successes, Failures
- Audit account logon events - Successes, Failures

7. Disable ipv6
8. Install antivirus on server 2003 (clamAV)
9. Perform virus scan (using windows defender for windows 7,2008,2012)
10. Enable view hidden folders
11. Monitor Logs
    - Event Viewer (IDs: 4624, 4778, 4670, 4660, 4656, 4663, 560),
    - TCPViewc https://do--/nixed sysinternals com/nibs/I'CPyi:w iiP
    - Process Explorer: heros://dQV/fjord lysine:rnals.com/b es ProcessExplorer,zie
    - netstat -b (admin required), netstat -ano

12. Group Policy(See windows 2003 checklist -) Security Options)
12. Scan computer with Windows Defender
13. Enable viewing hidden files/folders and full extensions.
12. Install Firefox and antivirus
13. Run windows updates (patch known exploits be before this)
- Using IE go to catalog.update.microsoft.com. Search for "KB# server 2003"
- then add to basket (make sure it is x64 if needed)
- 2003/2008 - KB958644 ; 2008 - KB975517 : All - KB2992611 , KB3011780
- Go to basket install all KB# updates

14. Remove VNC
    - http://www.gregorystrike.com/2012/02/29/script- to-uninstallremove-vnc-pa
15. Run Microsoft baseline security analyzer
    - Https://technet.microsoft.com/en-us/security/cc184924.aspx
16. Run security configuration wizard (built in)
17. Encrypt files if necessary. https://veracrypt.codeplex.com/

Active Directory

Authenticated Users and Everyone must not have these rights:
-Act as part of the operating system
-add workstations to domain '
-Backup files and directories
-Create a pagefile
-Create a token object
-Debug programs
-enable computer and user accounts to be trusted for delegation
-Force shutdown from a remote system
-increase quotas
-increase scheduling priority
-Load and unload device drivers
-Lock pages in memory
-Logon as a batch job
-Logon as a service
-Logon locally
-Manage auditing and security log
-Modify firmware environment variables
-Replace a process-level token
-Restore files and directories
-Shut down the system
- Synchronize directory service data
-Take ownership of files and other objects

Audit Policy Settings:

Audit account logon events, Audit account management, Audit directory service access, Audit logon events, Audit policy change, Audit privilege use: Success/Failure

Start -> Administrative Tools -> Local Security Policy ->Security'Settings ->Local Policies -> Audit Policy. To check this in DCs, go from Start -> Administrative Tools -> Domain Security Policy -> Security Settings -> Local Policies -> Audit poiicy. "
Event Log Settings:
Maximum security log size: 16384 kB
Prevent Local guests group from accessing security log: Enabled
Retain security log: Not defined
Retention method for security log: Overwrite events as needed

Start -> Administrative Tools -> local Security Policy -> Security Settings -> Event Log.
To check this in DCs, go from Start -> Administrative Tools -> Domain Security Policy -> Security Settings -> Event Log

To check their rights: Start -> Administrative Tools -> Local Security Policy -> Security Settings -> Event Log. To check this in DCs, go from Start -> Administrative Tools -> Domain Security Policy -> Security Settings -> Event Log.

Security Options to Enable:
-Accounts: Guest account status (Guest account should be disabled)
-Audit: Audit the use of backup and restore privilege
-Devices: Prevent users from installing print drivers
-Devices: Restrict floppy access to locally logged an user only
-Domain Member: Digitally encrypt or sign channel data (when possible)
-Domain member: Maximum password account password age
-Domain member: Require strong session key
-Interactive logon: Message text for users attempting to logon
-Interactive logon: Message title for users attempting to logon
-Interactive logon: Prompt user to change password before expiration
-Interactive logon: Require Domain Controller authentication to unlock workstation
-Microsoft network server: Amount of idle time required before suspending session
-Network access: Do not allow anonymous enumeration of SAM accounts and shares
-Network access: Restrict anonymous access to Named Pipes and Shares
-Network access: Sharing and security model for local accounts (Choose Classic-local users authenticate as themselves)
-Network security: Do not store LAN Manager hash value on next password change (choose Send NTLMv2 response only\refuse LM, but only if clients are all W2K/WXP)
-Network security: LAN Manager authentication level
-Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
-Shutdown: Clear virtual memory page file

-System cryptography: Force strong key protection for user keys stored on the computer
-System objects: Default owner for objects created by members of the Administrators group
-System objects: Require case insensitivity for non-Windows subsystems
-System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links')

MS SQL
Migrate to MYSQL using MYSQL Workbench's Migration Wizard

Patching
- Heartbleed
- ALL Security Updates for Windows Server 2003