**Windows starting Steps**

* Change password
* Create backup admin
* Turn on Firewall (2012 is in Control panel )
* Disable incorrect users on 2012
* Change user passwords.
* Check Services

<https://live.sysinternals.com/>

* + autoruns.exe
  + procexp.exe
  + Sysmon64.exe

**Install** – Command Prompt - Sysmon64.exe -accepteula -i

<https://www.malwarebytes.com/mwb-download/thankyou/>

**Turn off:**

Remote management

File Server remote management

Remote Management - Server manager 🡪 Local Server 🡪 Change Remote management to Disabled

Remote Desktop (should auto disable with Remote management )

Control panel 🡪 System and Security 🡪 System 🡪 Remote Settings on left 🡪 Change to “Don’t allow”

**File and print sharing**

Network and Sharing Center: - Turn off File and print Sharing  
  
Folder shares  
remove “everyone” from User share  
  
**List shares**

Get-SmbShare

Also can go to Computer Management 🡪 Shared folders 🡪 Shares

**Firewall**

?

Turn off File Server Remote Management ….

**SMB**

Check if SMB1 is enabled:

Get-SmbServerConfiguration | select EnableSMB1Protocol

Graphical user interface, text, website

Description automatically generated

If True, then run the following to disable SMB1:

Set-SmbServerConfiguration -EnableSMB1Protocol $false

Additional info:

check both SMB1 and SMB2

Get-SmbServerConfiguration | select EnableSMB1Protocol,EnableSMB2Protocol

Graphical user interface, text

Description automatically generated

To list the complete SMB configuration:

Get-SmbServerConfiguration   
Text

Description automatically generated

**Print Services**  
Open services, scroll to Print Spooler - Disable and stop Print Spooler

**Run in Command Prompt or Powershell**

Ipconfig /flushdns

**Add banner**

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\**

**LegalNoticeCaption -** UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

**LegalNoticeText -** You must have explicit, authorized permission to access or configure this device.

Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

Network connections

Netstat

To display active TCP connections and the process IDs every 5 seconds, type:

netstat -o 5

| **Parameter** | **Description** |
| --- | --- |
| -a | Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. |
| -b | Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions. |
| -e | Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**. |
| -n | Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names. |
| -o | Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**. |
| -p <Protocol> | Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be tcp, udp, tcpv6, or udpv6. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6. |
| -s | Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols. |
| -r | Displays the contents of the IP routing table. This is equivalent to the route print command. |

Add firewall port disable for port 80 and 443 to notes.

* netsh advfirewall firewall add rule name="Block TCP 80" dir=in protocol=tcp localport=80 action=block
* netsh advfirewall firewall add rule name="Block TCP 443" dir=in protocol=tcp localport=443 action=block

**Password policy**

GPEDIT.msc

Local Computer Policy 🡪 Computer Configuration 🡪 Windows Settings 🡪 Security Settings 🡪 Account Policy 🡪

Password Policy:

* Enforce password history 6
* Maximum Age 60
* Minimum Age 5
* Minimum length 12
* Enable Complexity

Local Computer Policy 🡪 Computer Configuration 🡪 Windows Settings 🡪 Security Settings 🡪 Account Policy 🡪 Account Lockout Policy:

* Account lockout threshold = 4
* Account lockout duration = 30

**Need to figure out a working NTP.**

**NTP**

w32tm /config /syncfromflags:172.20.240.20 /update

net stop w32time

net start w32time

**Configure NTP on Windows Server**

Open a command prompt.

Check time sync:

w32tm /query /source

If the output says Free-running System Clock or Local CMOS Clock, the server is not using NTP.

List NTP server list:

w32tm /query /peers

If the output shows that the peer list is empty and state pending, the server is not using NTP.

Update the peer list:

w32tm /config /update /manualpeerlist:SPACE\_LIMITED\_NTP\_SERVERS /syncfromflags:manual /reliable:yes

Force sync:

w32tm /resync /rediscover

Check if the server is now using NTP:

w32tm /query /source

If the output shows one of the servers in your peer list, the server is now using NTP.

Past note items

NTP Client  
Gpedit

Computer Configuration 🡪 Administrative template 🡪System 🡪 Windows Time Service 🡪 Time Providers

Enable Windows NTP Client on the right Pane. Enable

Configure NTP Client select Enable

NTPserver = 172.20.240.20

Type = NTP  
  
Test with net time /query sntp

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parametersregistry**