**First Steps:**

* Discuss README together
  + Mark important information about what you specifically need to do to the machine
* Get the flash drive.
  + If Service Packs are available Install them while discussing the README or after (WSUS offline Updater)
  + Download the Programs: MalwareBytes, BitDefender, CCleaner, IOBitUninstaller, MSBA, ProcessExplorer, and Wireshark.
  + Get your script for the machine you are working on.
  + Get the Internet Browsers that you are supposed to be running on your machine.
  + Get the Microsoft Common Console. (Shows services, shares, firewall, users + groups, event viewer, etc.)

**NOW FOR THE GOOD STUFF: Before Running script!!!**

* **ANSWER YOUR FORENSIC QUESTIONS!**
  + After, Open your Internet browser and make sure your Adobe Flash/Reader and Java Plugins are up-to-date. Also remove any toolbars that are not supposed to be there.

**Now for the script**

* If you have any question about the script ask the person who made it to make sure everything works correctly.
* After the script has ran take note of the things you have gotten points for if your script didn’t get point in a section it should have then you HAVE to check it manually.

**After script**

* Password Policy
  + Enforce password history: *24*
  + Maximum password age: *60*
  + Minimum password age: *1*
  + Minimum password length: *10*
  + Password must meet complexity requirements: *Enabled*
  + Store password using reversible encryption: *Disabled*
* Lockout Policy
  + Account lockout duration: *30 Minutes*
  + Account lockout threshold: *10*
  + Reset account lockout counter after: *30*
* Check user settings
  + All users should have ‘User must change password at next logon’ checked
  + All unauthorized users should have ‘Account is disabled’
* Check ALL the groups
  + ‘Administrators’ group should ONLY have AUTHORIZED admins.
  + ‘Guests’ group should ONLY have ‘Guest’ in it
  + If the README wants only certain users to use RDP then add ONLY those users to the ‘Remote Desktop Users’ group
* Use SmartScreen online services(Security and Maintenance)=ON
* Wi-Fi Sense (Network & Internet)
  + Automatically connect to suggested open hotspots=OFF
  + Automatically connect to hotspots temporarily to see if paid network services are available=OFF
* Turn UAC to max(Change User Account Control Settings)
* Change Adapter settings(Disabling IPv6 and other services)=Uncheck these
  + Client for MS Networks
  + File and Printer Sharing for Microsoft Networks
  + QoS
  + Microsoft Network Adapter Multiplexor Protocol
  + Microsoft LLDP Protocol Driver
  + Link Layer Topology Discovery Mapper IO Driver
  + Link Layer Topology Discovery Responder
  + Internet protocol version 6
  + 'Internet Protocol version 4 (TCP IPv4), click Properties, click Advanced,
  + 'DNS' tab, uncheck mark 'register this connections address in DNS'
  + 'WINS' tab, select 'Disable NETBIOS over TCP/IP'
* Disable port 1900 UPnP
  + Regedit path: HKLM\Software\Microsoft\DirectplayNATHelp\DPNHUPnP
  + Right click on right pane, new dword:32 bit, named UPnPMode
  + Double click on that and set it to 2
* Windows Services
  + UPnP Device Host: Stopped – Disabled
  + RDP: Depends on README
  + Telnet: Stopped – Disabled
  + SNMP Trap: Stopped – Disabled
  + Windows Event Collector: Running – Automatic
  + Remote Registry: Stopped - Disabled
  + ##ADD OTHER SERVICES
* Check windows features
  + Control Panel>Programs> Turn Windows features on or off
  + Things to never have on
    - Telnet client\server
    - SNMP
    - RIP Listener
    - Client for NFS
    - Internet Information Services (IIS)
    - World Wide Web Services
  + If FTP sever then turn on TFTP otherwise make sure that it is not checked
  + Disable SMB v1
    - Turn Windows features on or off=Uncheck SMB 1.0/CIFS File Sharing Support
* Shares
  + Only 3 shares should be shared unless README says otherwise
    - ADMIN$
    - C$
    - IPC$
* Firewall rules:
  + Inbound=disable MS Edge
  + Inbound=disable Search
  + Inbound=disable MSN Money
  + Inbound=disable MSN Sports
  + Inbound=disable MSN News
  + Inbound=disable MSN Weather
  + Inbound=disable Microsoft Photos
  + Inbound=disable Xbox
* Turning off Tiles:
  + Right click on the Tile and choose turn off
* Turn off AutoPlay
  + Settings..Devices….AutoPlay=off
* Run the command “netplwiz”
* Disable OneDrive on Startup
  + Use Task Manager or mscofig.exe
* Screen Saver
  + Settings…Personalize….Lock Screen...Screen Saver settings=wait 10 min and checkmark “On resume display Logon screen”
* Auditing
  + Change all to Success/Failure
* Windows defender
  + Turn on Windows defender
    - If disabled go into gpedit.msc and find the ‘windows defender’ option and change to enable
* User Rights Assignment

|  |  |  |
| --- | --- | --- |
| *Policy* | *Default* | *Secure Setting* |
| *Access Credential Manger as a trusted caller* | No one | No one |
| *Access the computer from the network* | Everyone, Administrators, Users, Backup Operators | Administrators |
| *Act as park of the operating system* | No one | No one |
| *Adjust memory quotas for a process* | Administrators, LOCAL SERVICE, NETWORK SERVICE | Administrators, LOCAL SERVICE, NETWORK SERVICE |
| *Allow log on locally* | Guest, Administrators, Users, Backup Operators | Administrators, Users |
| *Allow log on through Remote Desktop Services* | Administrators, Remote Desktop Users | Administrators, Remote Desktop Users |
| *Back up files and directories* | Administrators, Backup Operators | Administrators |
| *Change system time* | Administrators, LOCAL SERVICE | Administrators, LOCAL SERVICE |
| *Change the time zone* | Administrators, LOCAL SERVICE, Users | Administrators, LOCAL SERVICE, Users |
| *Create a pagefile* | Administrators | Administrators |
| *Create a token object* | No one | No one |
| *Create global objects* | Administrators, LOCAL SERIVCE, NETWORK SERVICE, SERVICE | Administrators, LOCAL SERIVCE, NETWORK SERVICE, SERVICE |
| *Create permanent shared objects* | No one | No one |
| *Create symbolic links* | Administrators | Administrators |
| *Debug programs* | Administrators | Administrators |
| *Deny access to this computer from the network* | Guest | Guest, Local account |
| *Deny log on as a batch job* | No one | Guest |
| *Deny log on as a service* | No one | Guest |
| *Deny log on locally* | Guest | Guest |
| *Deny log on through Remote Desktop Services* | No one | Guest, Local account |
| *Enable computer and user accounts to be trusted for delegation* | No one | No one |
| *Force shutdown from a remote system* | Administrators | Administrators |
| *Generate security audits* | LOCAL SERVICE, NETWORK SERVICE | LOCAL SERVICE, NETWORK SERVICE |
| *Impersonate a client after authentication* | Administrators, LOCAL SERIVE, NETWORK SERVICE, SERVICE | Administrators, LOCAL SERIVE, NETWORK SERVICE, SERVICE |
| *Increase scheduling priority* | Administrators | Administrators |
| *Load and unload device drivers* | Administrators | Administrators |
| *Lock pages in memory* | No one | No one |
| *Log on as a batch job* | Administrators, Backup Operators, Performance Log Users | Administrators |
| *Log on as a service* | NT SERVICE\ALL SERVICES | No one |
| *Manage auditing and security log* | Administrators | Administrators |
| *Modify an object label* | No one | No one |
| *Modify firmware environment values* | Administrators | Administrators |
| *Perform volume maintenance tasks* | Administrators | Administrators |
| *Profile single process* | Administrators | Administrators |
| *Profile system performance* | Administrators, NT SERVICE\WdiServiceHost | Administrators, NT SERVICE\WdiServiceHost |
| *Replace a process level token* | LOCAL SERVICE, NETWORK SERVICE | LOCAL SERVICE, NETWORK SERVICE |
| *Restore files and directories* | Administrators, Backup Operators | Administrators |
| *Shutdown the system* | Administrators, Backup Operators, Users | Administrators, Users |
| *Take ownership of file or other objects* | Administrators | Administrators |

* Local Security policies
  + **THESE ARE FOR MOST SECURE SETTINGS MAKE SURE TO CHECK THESE AS A TEAM!!!!!**
  + Accounts: Administrator account status*: disabled*
  + Accounts: Block Microsoft accounts: *Users can’t add or log on with Microsoft accounts*
  + Accounts: Guest account status: disabled \*\*
  + Accounts: Limit local account use of blank passwords to console logon only: *enabled*
  + Audit: Audit access of global system objects: *disabled*
  + Audit: Audit the use of Backup and Restore privilege: *disabled*
  + Audit: Force audit policy subcategory settings (Windows Vista of later) to override audit policy category settings: *enabled*
  + Audit: Shutdown system immediately if unable to log security audits: *enable?*
  + DCOM: Machine access restrictions: *no remote access for all accounts*
  + DCOM; Machine launch restrictions: *no remote launch and remote activation for all accounts*
  + Devices: Allow undock without having to log on: *disabled*
  + Devices: Allowed to format and eject removable media: *administrators and interactive users*
  + Devices: Prevent users from installing printer drivers: *enabled*
  + Domain member: Digitally encrypt or sign secure channel data (always): *enabled*
  + Domain member: Digitally encrypt secure channel data (when possible): *enabled*
  + Domain member: Digitally sign secure channel data (when possible); *enabled*
  + Domain member: Disable machine account password changes: *disabled*
  + Domain member: Maximum machine account password age: *30 days*
  + Domain member: Require strong (Windows 2000 or later) session key: *enabled*
  + Domain member: Display user information when session is locked: *do not display user information*
  + Interactive logon: Do not display last user name: *enabled*
  + Interactive logon: Do not require CTRL+ALT+DEL: *disabled*
  + Interactive logon; Machine account lockout threshold: *10 invalid logon attempts*
  + Interactive logon: Machine inactivity limit: *900 seconds*
  + Interactive logon: Number of previous logons to cache (in case domain controller is not available: *4 logons*
  + Interactive logon: Prompt user to change password before expiration: *14 days*
  + Interactive logon; Require Domain Controller authentication to unlock workstation; *Disabled*
  + Interactive logon: Require smart card: *disabled*..
  + Interactive logon: Smart card removal behavior: *Lock* *workstation*
  + MS network client: Digitally sign communications (always): *enabled*
  + MS network client: Digitally sign communications (if server agrees): *enabled*
  + MS network client: Send unencrypted password to third-party SMB servers: *disabled*
  + MS network server; Amount of idle time required before syspending session: *15* *minutes*
  + MS network server: Digitally sign communications (always): *enabled*
  + MS network server; Digitally sign communications (if client agrees); *enabled*
  + MS network server: Disconnect clients when logon hours expire: *enabled*
  + MS network server: Server SPN target name validation level: *Accept if provided by client*
  + 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*
  + Network access: Do not allow storage of passwords and credentials for network authentication: *enabled*
  + Network access: Let Everyone permissions apply to anonymous users: *disabled*
  + Network access: Named Pipes that can be accessed anonymously: *blank*
  + Network access: Remotely accessible registry paths: *blank*
  + Network access; Remotely accessible registry paths and sub-paths: *blank*
  + Network access: Restrict anonymous access to Named Pipes and Shares: *enabled*
  + Network access: Shares that can be accessed anonymously: *blank*
  + Network access: Sharing and security model for local accounts: *Classic - local users authenticate as themselves*
  + Network security: Allow Local System to use computer identity for NTLM: *enabled*
  + Network security: Allow LocalSystem NULL session fallback: *disabled*
  + Network security: Allow PKU2U authentication requests to this computer to use online identifies: *disabled*
  + Network security: Configure encryption types allowed for Kerberos: *RC4\_HMAC\_MD5, AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Future encryption types*
  + Network security: Do not store LAN Manager hash value on next password change: *enabled*
  + Network security: Force logoff when logon hours expire: *enabled*
  + Network security; LAN Manager authentication level: *Send NTLMv2 response only, Refuse LM & NTLM*
  + Network security: LDAP client signing requirements: *Negotiate signing*
  + Network security: Minimum session security for NTLM SSP based (including secure RPC) clients: *Require NTLMv2 session security, Require 128 bit encryption*
  + Network security: Minimum session security for NTLM SSP based (including secure RPC) server: *Require NTLMv2 session security, Require 128 bit encryption*
  + Network security: Restrict NTLM: Incoming NTLM traffic: *Deny all accounts*
  + Network security: Restrict NTLM: NTLM authentication in this domain: *Deny* *all*
  + Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers: *Deny* *all*
  + Recovery console: Allow automatic administrative logon: *disabled*
  + Recovery console: Allow floppy copy and access to all drives and all folders: *disabled*
  + Shutdown: Allow system to be shut down without having to logon: *disabled*
  + Shutdown: Clear virtual memory page-file: *disabled*
  + System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing: *disabled*
  + System objects: Require case insensitivity for non-Windows subsystems: *enabled*
  + System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links) : *enabled*
  + System settings: Optional subsystems: *blank*
  + System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies: *disabled*
  + UAC: Admin Approval Mode for Built-in Administrator account: *enabled*
  + UAC: Allow UIAccess applications to prompt for elevation without using the secure desktop: *disabled*
  + UAC: Behavior of elevation prompt for administrators in Admin Approval Mode: *Prompt for consent on the secure desktop*
  + UAC: Behavior of the elevation prompt for standard users: *Automatically deny elevation requests*
  + UAC: Detect application installations and prompt for elevation: *enabled*
  + UAC: Only elevate executables that are signed and validated: *disabled*
  + UAC; Only elevate UIAccess applications that are installed in secure locations: *enabled*
  + UAC: Run all administrators in Admin Approval Mode: *enabled*
  + UAC: Switch to the secure desktop when prompting for elevation: *enabled*
  + UAC: Virtualize file and registry write failures to per-user locations: *enabled*